

Military Police

Chemical Agent Security Program

Distribution Restriction Statement.
This publication contains technical or operational information that is for official Government use only. Distribution is limited to U.S. Government agencies. Requests from outside U.S. Government agencies for release of this publication must be made to Provost Marshal General, ATTN: (DAPM-MPD-PS), 2800 Army Pentagon, Washington, DC 20310–0400.

Destruction Notice.
Destroy by any method that must prevent disclosure of contents or reconstruction of the document.

**Headquarters
Department of the Army
Washington, DC
11 September 2006**

UNCLASSIFIED

SUMMARY of CHANGE

AR 190-59

Chemical Agent Security Program

This major revision, dated 11 September 2006--

- Designates the Headquarters, Department of the Army, Office of the Provost Marshal General with overall responsibility for the Department of the Army Chemical Agent Security Program and approving authority for waivers and exceptions to policy requirements (para 1-4c).
- Designates specific responsibilities for the Assistant Chief of Staff for Installation Management and the Installation Management Agency (para 1-4h).
- Assigns responsibilities to the Senior Mission Commander responsible for the overall security of the nuclear reactors and special nuclear material (para 1-4j).
- Establishes new requirements for requesting security deviations, with emphasis on compensatory measures, to include commander endorsements in chain of command (para 2-7).
- Designates the Provost Marshal General as approving authority for all security deviations (para 2-7e).
- Provides guidance on Department of the Army Implementing Instructions to the DOD Postulated Security Threat (para 3-2).
- Establishes new requirements for the conduct of vulnerability assessments (para 3-5).
- Establishes duties and responsibilities for the key control officer (para 8-4).
- Establishes duties and responsibilities for key custodians (para 8-5).
- Establishes a standardized format to document the results of vulnerability assessments (chap 16).
- Identifies members required to be on the vulnerability assessment team (para 16-4).
- Provides annotated outline/guidance for conducting initial vulnerability assessments (para 16-5).
- Provides annotated outline/guidance for conducting annual vulnerability assessment updates (para 16-6).

Effective 11 October 2006


Military Police

Chemical Agent Security Program

By Order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:


JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army

History. This publication is a major revision.

Summary. This regulation prescribes physical security policy, standards, and procedures for the Department of the Army Chemical Agent Security Program. It implements the security provisions in DOD Directive 5210.65.

Applicability. This regulation applies to all Active Army activities that have custody or possession of chemical agents, including Government-owned, Government-operated activities; Government-owned, contractor-operated activities; and contractor-owned, contractor-operated activities under Department of the Army

jurisdiction. It includes Government organizations, industry, and academia that use chemical agents under Government contracts for research and development or other authorized purposes. It does not apply to the U.S. Army Reserve or the Army National Guard/Army National Guard of the United States. This regulation is not applicable during full mobilization.

Proponent and exception authority.

The proponent for this regulation is the Office of the Provost Marshal General. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit, or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy

proponent. Refer to AR 25–30 for specific guidance.

Army management control process.

This regulation contains management control provisions in accordance with AR 11–2 but it does not identify key management controls that must be evaluated.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Office of the Provost Marshal General, ATTN: (DAPM–MPD–PS), 2800 Army Pentagon, Washington, DC 20310–2800.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Office of the Provost Marshal General, ATTN: (DAPM–MPD–PS), 2800 Army Pentagon, Washington, DC 20310–2800.

Distribution. This publication is available in electronic media only and is intended for command levels B, C, D, and E for the Active Army.

Distribution Restriction Statement.

This publication contains technical or operational information that is for official Government use only. Distribution is limited to U.S. Government agencies. Requests from outside U.S. Government agencies for release of this publication must be made to Provost Marshal General, ATTN: (DAPM–MPD–PS), 2800 Army Pentagon, Washington, DC 20310–0400.

Destruction Notice.

Destroy by any method that must prevent disclosure of contents or reconstruction of the document.

Contents (Listed by paragraph and page number)

Chapter 1

General, page 1

Purpose • 1–1, *page 1*

References • 1–2, *page 1*

Explanation of abbreviations and terms • 1–3, *page 1*

*This regulation supersedes AR 190–59, dated 1 July 1998.

Contents—Continued

Responsibilities • 1–4, *page 1*

Chapter 2

Security Measures, *page 2*

Requirement for extraordinary security measures • 2–1, *page 2*

Security forces and use of force • 2–2, *page 2*

Resources • 2–3, *page 3*

Physical security equipment • 2–4, *page 3*

General storage criteria • 2–5, *page 3*

Priority considerations • 2–6, *page 3*

Security criteria deviation program • 2–7, *page 4*

Investigations • 2–8, *page 5*

Two-person rule • 2–9, *page 6*

Chapter 3

Security planning (policy), *page 6*

Threat considerations • 3–1, *page 6*

DA Implementing Instructions to the DOD Postulated Threat • 3–2, *page 6*

Security planning factors • 3–3, *page 6*

Additional planning requirements • 3–4, *page 6*

Vulnerability assessments • 3–5, *page 6*

Security planning assistance • 3–6, *page 6*

Tactical defense plan • 3–7, *page 7*

Coordination and integration of plans • 3–8, *page 7*

Classification of plans • 3–9, *page 7*

Physical security plan outline • 3–10, *page 7*

Chapter 4

Perimeter Security, *page 10*

Category I and II Chemical agents • 4–1, *page 10*

Perimeter security system • 4–2, *page 10*

Perimeter boundary fencing • 4–3, *page 10*

Clear zones • 4–4, *page 11*

Security lighting • 4–5, *page 12*

Entry control facilities • 4–6, *page 12*

Perimeter detection and assessment system • 4–7, *page 13*

Restricted area designation • 4–8, *page 13*

Perimeter defensive positions • 4–9, *page 13*

Vehicle barriers • 4–10, *page 14*

Security during construction projects • 4–11, *page 14*

Limited area topography • 4–12, *page 14*

Chapter 5

Storage Requirements, *page 14*

Category I or II chemical agents • 5–1, *page 14*

Bulk storage • 5–2, *page 14*

Locking systems • 5–3, *page 15*

Storage structure entry hindrance • 5–4, *page 16*

Security construction verification • 5–5, *page 16*

Binary precursors • 5–6, *page 16*

Interior and exterior IDS requirements • 5–7, *page 16*

Chapter 6

Support Facilities, *page 19*

Category I or II chemical agents • 6–1, *page 19*

Contents—Continued

Site Security Control Center • 6–2, *page 19*

Power sources • 6–3, *page 19*

Communications • 6–4, *page 19*

Maintenance requirements • 6–5, *page 20*

Chapter 7

Security Procedures, *page 20*

Category I or II chemical agents • 7–1, *page 20*

Entry controls • 7–2, *page 20*

Visitor controls • 7–3, *page 23*

Package, material, and vehicle controls • 7–4, *page 23*

Opening of storage structures after duty hours • 7–5, *page 23*

Security of open igloos • 7–6, *page 23*

Chemical Weapons Treaty Compliance Inspections • 7–7, *page 24*

Chapter 8

Key and Lock Controls, *page 25*

Category I, II, or III chemical agents • 8–1, *page 25*

Access and controls • 8–2, *page 25*

Lock rotation • 8–3, *page 26*

Key control officer • 8–4, *page 27*

Key custodian • 8–5, *page 27*

Chapter 9

Security Forces, *page 27*

Category I or II chemical agents • 9–1, *page 27*

Qualifications of security force personnel • 9–2, *page 27*

Guard motivation requirements • 9–3, *page 28*

Guard orders • 9–4, *page 28*

Security forces and use of Force • 9–5, *page 28*

Response force • 9–6, *page 28*

Augmentation force • 9–7, *page 29*

Records of test exercises • 9–8, *page 30*

Security force weapons and equipment • 9–9, *page 30*

Tactical defense deployment • 9–10, *page 30*

Site area searches • 9–11, *page 31*

Operations security • 9–12, *page 31*

Site and perimeter patrols • 9–13, *page 31*

Control of demonstrations • 9–14, *page 31*

Tactical deployment in response to alarms • 9–15, *page 31*

Unannounced aircraft landings • 9–16, *page 32*

Guard logs • 9–17, *page 32*

Chapter 10

Training, *page 32*

Category I and II chemical storage sites • 10–1, *page 32*

Training requirements • 10–2, *page 32*

Basic training program. • 10–3, *page 32*

Specialized training • 10–4, *page 33*

Continuing training • 10–5, *page 33*

Training records • 10–6, *page 34*

Force-on-force training • 10–7, *page 34*

Weapons training • 10–8, *page 34*

Training evaluation • 10–9, *page 34*

Contents—Continued

Chapter 11

Transportation Security, page 34

All categories of chemical agents • 11–1, *page 34*

Off-post movement of chemical agents in quantities greater than category III • 11–2, *page 34*

Off-post and on-post movements of category III chemical agents • 11–3, *page 35*

On-post movements of category III or greater chemical agents between limited areas involving chemical demilitarization operations • 11–4, *page 35*

Movements of recovered chemical warfare materials • 11–5, *page 35*

Requests for additional security guidance • 11–6, *page 35*

Chapter 12

Chemical Agent Recapture and Recovery Operations Planning, page 35

All categories of chemical agents • 12–1, *page 35*

Procedures • 12–2, *page 35*

Planning • 12–3, *page 35*

Secure voice radio • 12–4, *page 36*

Chapter 13

Category III RDTE Chemical Agents at On Post Locations, page 36

Category III RDTE chemical agent general requirements • 13–1, *page 36*

Limited/exclusion areas • 13–2, *page 36*

Vulnerability assessment • 13–3, *page 36*

Storage containers • 13–4, *page 36*

Rooms or laboratories • 13–5, *page 37*

Exterior doors of buildings • 13–6, *page 37*

Security construction verification • 13–7, *page 37*

Security lighting • 13–8, *page 37*

Intrusion detection system (IDS) • 13–9, *page 37*

Security forces • 13–10, *page 38*

Two-person rule • 13–11, *page 39*

Key and lock controls • 13–12, *page 39*

Entry controls • 13–13, *page 39*

Package and material control • 13–14, *page 39*

End of day security checks • 13–15, *page 39*

Opening of room or laboratory after duty hours • 13–16, *page 40*

Security inspections • 13–17, *page 40*

Recapture and recovery operations • 13–18, *page 40*

Physical security plans • 13–19, *page 40*

Transportation • 13–20, *page 40*

Chapter 14

Security Provisions for Contracts and Agreements Involving Category III RDTE Chemical Agents at Off Post Locations, page 40

Category III RDTE chemical agents • 14–1, *page 40*

Limited and exclusion areas • 14–2, *page 40*

Vulnerability assessment • 14–3, *page 40*

Storage/containers • 14–4, *page 41*

Rooms and laboratories • 14–5, *page 41*

Exterior doors of buildings • 14–6, *page 42*

Security construction verification • 14–7, *page 42*

Security lighting • 14–8, *page 42*

Intrusion detection system (IDS) • 14–9, *page 42*

Security response forces • 14–10, *page 43*

Communications and duress system • 14–11, *page 43*

Two-person rule • 14–12, *page 43*

Contents—Continued

- Key and lock controls • 14–13, *page 43*
- Key control officer and key custodians • 14–14, *page 45*
- Entry controls • 14–15, *page 45*
- Package and material controls • 14–16, *page 45*
- End of day security checks • 14–17, *page 45*
- Opening of room or laboratory after working hours • 14–18, *page 45*
- Security inspections • 14–19, *page 45*
- Duration of security provisions • 14–20, *page 46*
- Chemical agent recapture and recovery plan • 14–21, *page 46*
- Reporting security incidents • 14–22, *page 46*
- Physical security plan • 14–23, *page 46*
- Physical security plan outline • 14–24, *page 46*

Chapter 15

Chemical Demilitarization Processing Operations, *page 48*

- All categories of chemical agents • 15–1, *page 48*
- Movement of chemical agents to chemical DEMIL processing facilities • 15–2, *page 48*
- Chemical DEMIL processing facilities • 15–3, *page 48*
- Storage/Staging limitations • 15–4, *page 49*
- Security of doors and windows • 15–5, *page 50*
- Locking systems • 15–6, *page 50*
- Key and lock controls • 15–7, *page 50*
- Interior IDS • 15–8, *page 50*
- Monitoring of IDS and CCTV • 15–9, *page 50*
- Entry and exit controls • 15–10, *page 51*
- Security forces • 15–11, *page 51*
- Integration of security posture • 15–12, *page 51*

Chapter 16

Conduct of Vulnerability Assessments and Documentation, *page 51*

- All categories of chemical agents • 16–1, *page 51*
- The DA Implementing Instructions to the DOD Postulated Threat • 16–2, *page 51*
- Conduct of vulnerability assessment and reviews • 16–3, *page 51*
- VA team composition • 16–4, *page 51*
- Annotated outline/guidance for conducting initial VA • 16–5, *page 52*
- Annotated outline/guidance for conducting annual VA reviews and updates • 16–6, *page 53*

Chapter 17

Protective Purposes Production Facility (PPPF) Category III Chemical Defense Training Facility (CDTF), *page 53*

- Category III CDTF chemical agent general requirements • 17–1, *page 53*
- Limited/exclusion areas • 17–2, *page 54*
- Vulnerability assessment • 17–3, *page 54*
- Storage containers • 17–4, *page 54*
- Laboratory (limited area) • 17–5, *page 54*
- Exterior doors of buildings • 17–6, *page 54*
- Security construction verification • 17–7, *page 54*
- Perimeter security • 17–8, *page 54*
- Clear zones • 17–9, *page 55*
- Security lighting • 17–10, *page 55*
- Site Access Center (SAC) • 17–11, *page 56*
- Perimeter detection and assessment system • 17–12, *page 56*
- Restricted area designation • 17–13, *page 56*
- Intrusion detection system (IDS) • 17–14, *page 56*
- Security forces • 17–15, *page 57*

Contents—Continued

Key and lock controls • 17–16, *page 58*

Entry controls • 17–17, *page 58*

Chemical Agent Recapture and Recovery Operations Planning • 17–18, *page 58*

Appendix A. References, *page 60*

Glossary

Chapter 1

General

1-1. Purpose

This regulation—

- a.* Prescribes policies, procedures, and minimum standards for the physical security of category I, II, and III chemical agents, as defined in AR 50-6, in the custody, possession, or jurisdiction of the Army.
- b.* Follows the basic chemical agent surety policy in AR 50-6 in establishing the physical security requirements for chemical agents in this regulation.
- c.* Prescribes physical security measures to prevent sabotage, theft, loss, seizure, or unauthorized access or use of chemical agents.
- d.* Applies to storage and transportation of chemical agents, regardless of location.

1-2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1-3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

1-4. Responsibilities

a. The Assistant Secretary of the Army, Installation and Environment (ASA (I&E)), has the principal responsibility for all DA programs relating to installations, real estate, chemical agent destruction, environment, safety, and occupational health. The ASA (I&E) will provide strategic direction, determine objectives, establish policy, set standards, and propose programming and funding for these programs.

b. The Assistant Secretary of the Army for Acquisitions, Logistics, and Technology (AL&T) will ensure physical security requirements are considered early during the research, development, and acquisition (RDA) of chemical agents.

c. The Provost Marshal General (DAPM-MPD-PS) has overall Army Staff (ARSTAF) responsibility for the DA Chemical Agent Security Program. The Chief, Operations Division, Office of the Provost Marshal General, (DAPM-MPD) will—

- (1) Establish overall policy for the physical security aspects of the program.
- (2) Function as the ARSTAF focal point for physical security matters.
- (3) Prepare DA Implementing Instructions to the DOD Postulated Threat to chemical agents.
- (4) Establish minimum physical security standards, criteria, and procedures for protecting chemical agents.

d. The Director, Strategy, Plans, and Policy (DAMO-SS), G-3, will provide the overall surety policy and guidance for the Army Chemical Surety Program.

e. The Deputy Chief of Staff, G-2 (DCS, G-2) will—

- (1) Publish an annual threat statement.
- (2) Coordinate with Commanding General (CG), U.S. Army Criminal Investigation Command (USACIDC) for inclusion on domestic threat information.
- (3) Maintain current, evaluated information concerning the hostile intelligence and terrorist threats to the security of chemical agents and disseminate the information to the responsible commanders and law enforcement officials.

f. The Chief of Engineers (COE) will ensure that the construction plans for new or modified chemical facilities meet the minimum standards prescribed in this regulation.

g. The Commanding General (CG), U.S. Army Criminal Investigation Command (USACIDC) will—

(1) Maintain current, evaluated information concerning the criminal threat to the security of chemical agents and disseminate the information to the responsible commanders and law enforcement officials, as appropriate.

(2) Conduct preliminary investigations into losses or recovery of chemical agents, regardless of dollar value, to determine if criminal misconduct occurred.

(3) Conduct investigations of actual or attempted break-ins or armed robberies of chemical agent storage facilities and theft of chemical agents in-transit. Monitor investigations conducted by civil law enforcement agencies when such incidents involve in-transit movements of chemical agents that are not under military control.

(4) Provide copies of USACIDC reports of investigations (ROI) or a letter reflecting the results of investigations which are prepared pertaining to (2) and (3), above, to ATTN: Office of the Provost Marshal General, (DAPM-MPD-PS), 2800 Army Pentagon, Washington, DC 20310-2800. Copies of ROIs prepared by civil law enforcement agencies will be obtained for military use, as required.

(5) Using the results of completed investigations, crime prevention surveys, or provost marshal physical security inspections, assist HQDA (DAPM-MPD-PS) and the commander concerned in evaluating existing security measures and recommending corrective action to improve security of chemical agents.

- (6) Provide Army G-2 domestic threat information for inclusion in the annual threat statement.
- h.* The Commander, Installation Management Agency (IMA) will—
 - (1) Provide oversight of garrison support to the chemical facilities commander/director.
 - (2) Provide assistance to the mission commander in resolving chemical agent related issues of support from the garrison commander.
- i.* The Commanding General, Forces Command (CG, FORSCOM) will, in coordination with MACOM Commanders/Senior Mission Commanders with a chemical mission, provide an augmentation force to support security forces at chemical agent facilities covered by this regulation.
- j.* The Senior Mission Commander (SMC) is responsible for the overall security of chemical agents and will—
 - (1) Establish and maintain a command chemical agent security program consistent with this regulation.
 - (2) Designate a physical security officer as focal point for the chemical agent physical security program.
 - (3) Assess subordinate organizations for compliance with applicable physical security regulatory requirements.
 - (4) Provide command oversight, direction, guidance, and assistance as necessary to ensure compliance with the provisions of this regulation.
 - (5) Plan, program, budget, and allocate for the implementation of physical security requirements in this regulation.
 - (6) Ensure current intelligence threat information is provided to facility commanders/directors, to include the DA Implementing Instructions to the DOD Postulated Threat.
 - (7) Conduct physical security inspections/surveys of chemical agent facilities and related facilities in accordance with appropriate regulations.
 - (8) Develop the site vulnerability assessment procedures and standardized format for documenting the assessment and after action results.
 - (9) Publish plans for the recovery of lost, seized, or stolen chemical agents.
- k.* Garrison commanders will support tenant chemical facilities by providing the necessary response force when required and/or supplement the facility's response force when requested by the chemical facility commander/director.
- l.* Commanders, directors, and custodians of chemical agent facilities will—
 - (1) Ensure positive measures are taken for the complete physical security control of chemical agents during all phases of their life cycle.
 - (2) Implement plans for the recovery of seized, stolen, or lost chemical agents.
 - (3) Immediately report incidents and threats related to sabotage, seizure, theft, or loss of chemical agents (actual or suspected) to the HQDA Army Operations Center (AOC) or through the most expeditious means available. Provide facts and circumstances in writing as soon as possible to HQDA Provost Marshal General (DAPM-MPD-PS), 2800 Army Pentagon, Washington, DC 20310-2800.
 - (4) Ensure timely submission of Serious Incident Reports (SIR) according to requirements in AR 190-40.
 - (5) Conduct prompt investigations per AR 15-6 of losses or recovery of chemical agents following a decision by the USACIDC that criminal acts were not involved.
 - (6) Ensure a formal site physical security plan and vulnerability assessment (VA) are conducted at each facility and revised annually or more frequently as new vulnerabilities become apparent. Provide a copy of the completed VA and updates and physical security plan through command channels to the appropriate SMC and to the garrison commander.

Chapter 2 Security Measures

2-1. Requirement for extraordinary security measures

- a.* Chemical agents are inherently dangerous, potentially lethal, and are possible targets for theft, sabotage, or unauthorized use. Public confidence in the Army's ability to protect its chemical agents against unauthorized access is also of concern. It is essential that frequent and periodic security assessments are made of the potential threat, the chemical agent's environment, and the risks and vulnerabilities associated with the chemical agents.
- b.* Assessing the adequacy of the security of chemical agents will be an essential task for the responsible commander. The DA Implementing Instructions to the DOD Postulated Threat to chemical agents, DA and SMC annual threat statements, local threat, and all other relevant factors will be considered. Security programs and procedures will be revised accordingly to ensure adequate protection of chemical agents at all times.
- c.* Physical security procedures must constitute a balanced, in-depth system responsive to all credible and potential threats and vulnerabilities.

2-2. Security forces and use of force

- a.* There will be sufficient security forces assigned and designated to provide necessary security requirements outlined in this regulation. Security forces will be organized, trained, armed and equipped to provide normal day-to-day

protection for chemical agents and to react to security incidents involving chemical agents. Response times for security personnel will be adjusted to ensure prompt assessment and responses of sufficient personnel in time to deny access to facilities containing chemical agents. Assessing the adequacy of the security of chemical agents will be an essential task for the responsible commander. The DA Implementing Instructions to the DOD Postulated Threat to chemical agents, local threat, intelligence, and all other relevant factors will be considered. Security programs and procedures will be revised accordingly to ensure adequate protection of chemical agents at all times. Threat analyses or other security considerations may lead to a doubt that adequate protection can be provided for chemical agents from available resources. If so, commanders will request appropriate assistance through command channels.

b. In accordance with AR 190–14, chemical agents are designated as inherently dangerous to others. Security forces will be armed and all possible actions will be taken, including the use of deadly force within the limitations of AR 190–14, to prevent the actual theft or sabotage of chemical agents.

c. Unauthorized personnel will not be permitted to control, remove, or otherwise compromise chemical agents. Every means available, to include the use of deadly force, if required, will be used to prevent actual theft, sabotage, or seizure of any chemical agent and recover immediately chemical agents wrongfully taken from their proper custody.

d. Ensure immediate re-occupation and security of a chemical agent exclusion area wrongfully penetrated.

2–3. Resources

Commanders at all levels will apply sufficient human resources and funds to the DA Chemical Agent Security Program to ensure a secure environment for chemical agents. SMC commanders will identify resource needs in the planning, programming and budgeting system, and allocate necessary resources to support their chemical agent security programs. Commanders will ensure funds identified for physical security are used as intended.

2–4. Physical security equipment

Guidance in AR 190–13 will be followed for the planning, evaluation, approval, and procurement of physical security equipment, which includes any item, device, or system used to protect chemical agents.

2–5. General storage criteria

a. The provisions of this regulation are mandatory for all new construction of permanent chemical agent storage facilities, to include demilitarization processing facilities. However, the tearing down and rebuilding of facilities and systems will not be undertaken unless there has been a determination by the SMC that existing physical security measures cannot be supplemented to provide the required degree of protection prescribed in this regulation.

b. The following minimum standards will apply for storage criteria of chemical agents:

(1) Storage sites will be consolidated to the maximum extent possible consistent with military operational planning factors.

(2) Each storage site will be as small as possible consistent with operational and safety considerations.

(3) Chemical agents will not be collocated in a storage structure with unrelated materiel such as non-chemical arms, ammunition, and explosives, other than as components of a complete round.

(4) All chemical agents will be stored in enclosed storage structures.

(5) All chemical agents will be secured to prevent sabotage, theft, loss, seizure, or unauthorized access or use of chemical agent.

(6) Chemical agents will be stored in exclusion areas within limited areas. Removal from a limited area is authorized only when required for operational or emergency conditions, or when transported according to requirements in AR 50–6.

c. The security requirements of this regulation apply to Army-managed contract operated facilities involving DOD provided chemical agents. This paragraph applies to any new contract or extension to an existing contract that occurs after the effective date of this regulation.

(1) Army chemical agent security requirements will be implemented by contractually binding agreements.

(2) The Contracting Officer will designate a Contracting Officer Representative to monitor chemical agent contracts. Contracting Officers will ensure that Army Chemical Agent Security Clauses are contractually binding on all Army contractors required to possess or use DOD or Army furnished chemical agents to include other Government organizations, industry or academia under U.S. Army contracts for research and development (or other authorized purposes).

(4) The Army will not furnish chemical agents until a contractor's facility demonstrates compliance with the chemical agent security contract clause(s) based on a review conducted by the responsible SMC. The responsible SMA will conduct periodic security reviews of contractor facilities for compliance with security contract requirements. If possible, these reviews will be conducted in conjunction with Surety Management Reviews (SMR).

2–6. Priority considerations

SMC s will prioritize physical security requirements according to the category of the chemical agents (see AR 50–6). The requirements will be listed in priority sequence by category for planning, programming, and budgeting.

2-7. Security criteria deviation program

a. Purpose. The purposes of the chemical agent security criteria deviation program in this regulation are to—

(1) Ensure that prescribed security requirements are properly observed and implemented at all activities where chemical agents are stored.

(2) Be used as a management tool to monitor corrective actions taken to ensure established security requirements are maintained.

(3) Ensure that deviations from established security requirements are systematically and uniformly identified and approved by the proper level of command so that compensatory measures are taken where necessary.

b. Deviation categories. A deviation from a specific security requirement prescribed in this regulation will be categorized as either a waiver or exception.

(1) *Waiver.* A waiver may be approved for temporary relief from a specific requirement prescribed in this regulation pending actions to conform to the requirement. Compensatory security measures will be required. A waiver may be approved for a period not to exceed 24 months, and may be extended only after a review of the circumstances that necessitate the extension. Compensatory measures approved by the local commander/director will remain in effect pending formal review and final approval by the approving authority. Deficiencies that will be corrected within 60 days will not require a waiver; however, compensatory security measures will be taken during the interval and communicated to all personnel concerned. In such cases, the compensatory measures will be in writing, approved by the local commander/director.

(2) *Exception.* An exception may be approved for permanent relief from a specific requirement prescribed in this regulation. Compensatory security measures will be required. Exceptions may be approved only when correction of the deviation is adjudged to be not feasible or cost-effective, and only after a most careful and critical evaluation of the facts in the case. The approving authority will be notified through command channels when the exceptions are no longer needed. All exceptions and waivers will be reviewed during periodic physical security inspections and surveys to ensure established compensatory measures are still valid and being followed. The results of these reviews will be documented and maintained locally for the duration of the exception.

c. Limitations. The following limitations apply—

(1) Exceptions and waivers will not be used to reduce or eliminate the minimum security requirements in this regulation.

(2) Each waiver or exception will be evaluated and approved on a case-by-case basis. Requests for waivers and exceptions that address identical requirements for deviation at more than one facility may be approved on a case-by-case basis.

d. Compensatory measures. The following requirements apply—

(1) Compensatory measures will be instituted for each deficiency.

(2) If appropriate, one compensatory measure may suffice for more than one deficiency.

(3) Security measures will compensate for the specific vulnerability created by the deficiency. A vulnerability is presumed to have been created when a minimum security requirement in this regulation cannot be met. A security requirement directed by this regulation cannot serve as a compensatory measure for a deficiency.

(4) Compensatory measures may include additional security forces, procedures, and/or physical security devices such as additional locks, alarms, lighting, camera surveillance devices and delay devices. The criteria for accepting compensatory measure will be designed to specifically enhance the security posture in light of the deficient situation.

(5) Compensatory measures which consist primarily of instructions to the security force to increase their alertness do not provide a comparable level of security.

(6) In the case of chemical sites that do not have installed perimeter IDS, or are not scheduled for installation of perimeter intrusion detection system (IDS), a thorough documented assessment will be made to determine the compensatory measures that would be most reasonable in light of the necessity to ensure near-real time assessment of attempted perimeter intrusions. The assessment will include a full explanation of the factors considered in formulating the compensatory measures in the context of the security objectives and vulnerabilities associated with protecting a chemical storage perimeter. The efficient use of all assigned security force personnel will be considered to satisfy the intent of this requirement. In this regard, the assessment will provide details showing the authorized and actual manpower strength of security force organizations and how these personnel are utilized efficiently on a daily basis. Show how the proposed compensatory measures are supported by the site security system (that is, system of defense in depth or upon accumulated delay time which protect storage structures or areas containing chemical agents). Follow procedures in *f*, below, to obtain approval for exceptions.

(7) In the case of compensatory measures for the response force reaction time at RDTE facilities (chaps 13 and 14), a thorough documented assessment will be made of the construction design of the particular facility to determine the estimated forced entry delay time of intruders described in the DOD postulated threat for RDTE facilities. The first defense layer against forced entry is the exterior of the building containing the chemical agents. The second defense layer is the shell of the chemical agent rooms or laboratories (walls, doors, floors, ceilings, and utility openings). The third defense layer is the chemical container. Document the forced entry delay times. Show how the forced entry delay times will preclude unauthorized access to the chemical agents prior to the arrival of the security force.

(8) A 10-percent deviation from all measurable standards, such as clear zone distances, fence height, and so forth, is permitted. Therefore, such deviation does not require the submission and approval of a waiver or exception request. Compensatory measures will be required when two or more 10-percent deviations, taken together, are determined to constitute a vulnerability in the site security system. For example, a fence that is a few inches below the required height does not, by itself, constitute a vulnerability; therefore, no compensatory measures are necessary. However, if there are additional 10-percent deviations at the storage facility, for example, clear zones and perimeter lighting, which taken together, are determined to create a vulnerability, then compensatory measures are required. Ten-percent deviations will be documented in the site security plan. Required compensatory measures for 10-percent deviations will be approved by the local commander.

(9) Security force considerations are as follows:

(a) Commanders and security managers will ensure that prescribed compensatory measures are implemented as required.

(b) Security forces will be made aware of the deviations and required compensatory measures currently in effect in the area where they are assigned.

(c) Prescribed compensatory measures for individual deficiencies must not, when considered in total, unrealistically task the security forces in the area where they are assigned.

e. Approving Authority. The Office of the Provost Marshal General will be the approving authority for waivers and exceptions to policy requirements in this regulation.

f. Commander's evaluation of the requests. Commanders (in the chain of command) will review and endorse each waiver or exception request. At the Major Subordinate Command (MSC) and SMC level, commanders may delegate the review and endorsement to a Senior Executive Service civilian assigned to that headquarters who is responsible for physical security matters in the command. Each chain of command's endorsement will include comments assessing the adequacy of compensatory measures, taking into consideration the required criteria for waivers and exceptions.

g. Procedures to obtain approval. Requests for waivers or exceptions should be initiated by the commander of the site or activity involved and forwarded in writing through command channels to the appropriate approving authority. Requests for HQDA will be forwarded through command channels to ATTN: HQDA OPMG (DAPM-MPD-PS), 2800 Army Pentagon, Washington, DC 20310-2800. As a minimum, all waiver and exception requests will include the following information—

(1) *Subject of request.* (for example, Request for Waiver at Pine Bluff Arsenal).

(2) *Reasons for request.* State the problems or deficiencies that constitute requirements below those cited in this regulation (cite references and state requirements).

(3) *Reasons for noncompliance.* Provide the following information—

(a) Explain why the unit, facility, or installation cannot comply with the requirements of this regulation.

(b) Show what action has been taken planned or scheduled, to correct the deficiencies. If corrective action is planned or scheduled, give specifics, to include anticipated date of completion.

(4) *Compensatory measures.* Provide detailed information concerning the compensatory measures in effect.

(5) *Adequacy of compensatory measures.* Show that the adequacies of the stated compensatory measures have been considered in light of the risks and threats to chemical agents.

(6) *Coordination.* Show that the request for waiver or exception has been coordinated with affected staff agencies and identify them. As a minimum, requests will be coordinated with the provost marshal (or equivalent official), supporting judge advocate of the installation or activity, when applicable, and supporting engineer when structural deviations are involved.

h. Commander's evaluation of requests. Commanders in the chain of command will review and endorse each waiver or exception request to ensure that adequate compensatory measures have been established. At the MACOM and MSC level, commanders may delegate this review and endorsement to a General Officer or Senior Executive Service (SES) civilian assigned to the headquarters responsible for physical security matters within the command.

i. Classification. Information contained in requests for waivers and exceptions may require appropriate security classification according to criteria in AR 380-86 (for example, critical vulnerabilities).

j. Status of current waivers and exceptions. Waivers and exceptions granted under the provisions of superseded AR 190-59, 01 July 1998, will continue to be valid after the publication date of this regulation, unless sooner cancelled or expired.

2-8. Investigations

a. The chemical agent facility Commander/Director will notify the supporting LEA, PM, or Security Office immediately upon discovery of suspected theft or loss of chemical agents. The notification will be as complete as possible but will not be delayed due to incomplete information.

b. The supporting law enforcement or security office will notify HQDA in accordance with the serious incident reporting (SIR) procedures in AR 190-40. Notification will also be made to the supporting USACIDC office in accordance with AR 5-9.

c. USACIDC will conduct an investigation to determine possible criminal misconduct. USACIDC will contact the

appropriate FBI if determined necessary. Should USACIDC determine no crime was committed, the custodial commander/Director will request an investigation in accordance with AR 15–6.

2–9. Two-person rule

Access to chemical agents will be controlled according to the two-person rule (see glossary) requirements in AR 50–6.

Chapter 3 **Security planning (policy)**

3–1. Threat considerations

Site security planning will consider the risk and threat factors associated with chemical agents (para 3–2).

3–2. DA Implementing Instructions to the DOD Postulated Threat

a. The DA Implementing Instructions to the DOD Postulated Threat will be implemented in security planning to prevent the sabotage, theft, loss, seizure, or unauthorized access or use of chemical agents.

b. Commanders will be responsible for the development of specific, validated threat assessments. They will request input from their local law enforcement and intelligence communities.

c. The DA Implementing Instructions to the DOD Postulated Threat has been distributed to affected Senior Mission Commanders (SMC) and The Surgeon General. Updates will be provided as necessary. SMC and The Surgeon General will provide a copy of the DA Implementing Instructions to the DOD Postulated Threat to each commander/director responsible for the security of chemical agents in the custody, possession, or jurisdiction of the Army, to include contract facilities, regardless of location.

3–3. Security planning factors

The security system at chemical agent storage facilities should assist the security forces in—

- a.* Preventing innocent or inadvertent penetration.
- b.* Assuring a capability for positive detection, identification, interception, and prevention of any unauthorized access to chemical agents. The security system should be designed to ensure the security force is capable of early detection and apprehension of intruder(s) before they gain access to the chemical agents.
- c.* Providing complete, positive, and efficient control of authorized entry into the storage area to the chemical agents.
- d.* Assuring expeditious entry of emergency forces such as fire department, explosive ordnance disposal, security, and response force (RF) personnel.

3–4. Additional planning requirements

The following additional security planning requirements apply, as applicable—

- a.* AR 190–13 provides requirements to be considered when developing physical security programs.
- b.* AR 525–13 provides requirements for protecting Army personnel and assets from terrorist attacks and for responding to terrorist attacks, if deterrence fails.

3–5. Vulnerability assessments

a. Vulnerability assessments (VAs) will be conducted at each chemical agent facility to identify and counter vulnerabilities which impact on the security of chemical agents. Requirements in Chapter 16 apply.

b. The results of the VAs will be used to prepare or update physical security plans and procedures.

3–6. Security planning assistance

The Office of the Chief of Engineers, HQDA, and SMC will provide necessary assistance for security planning, including the planning, design, and construction of storage sites or facilities.

a. A physical security plan will be prepared for each storage site, facility, or area containing chemical agents.

b. The physical security plan will be prepared according to the physical security plan outline in paragraph 3–10. The outline may be modified as necessary to facilitate use of the plan, but all applicable requirements prescribed by this regulation will be covered.

c. The plan will be signed by the site commander. The plan will be updated as required and formally reviewed with appropriate changes made at least annually.

d. The next higher commander/director will formally review and approve the plan and any changes. Such reviews will be recorded and signed by the approving authority (commander, deputy commander, or chief of staff).

e. The Physical Security Plan is a living document. Therefore, minor procedural and administrative updates (that is, minor changes in procedures, and so forth) will be reviewed and approved by the site commander/director or his/her

designated representative. These updates will be formalized in the plan and forwarded to the next higher commander when the plan is due for annual review.

f. Required portions of the plan may be kept as part of other planning documents, for example, disaster control plans, chemical surety plans, and so forth, but must be made available for review and use.

3-7. Tactical defense plan

a. A tactical defense plan will be prepared for each storage site of chemical agents in bulk storage areas (Categories I and II). The following guidance applies:

- (1) The plan will be developed and prepared after the site vulnerability assessment is completed.
- (2) The plan will follow the operation order format outlined in Field Manual 5-0.
- (3) The plan will be attached as an annex to the site physical security plan.
- (4) The plan will depict the scheme of maneuver, fields of fire, and defensive positions of security forces involved in the operation. It will also include tactical actions to repel attacks by airborne or air assault forces. The rules of engagement will be included in all tactical considerations.

b. The plan will be tailored to the local known threat, postulated threat to chemical agents, and site environment. As the threat changes, the plan will be reevaluated and changed as necessary to ensure adequate protection.

c. The plan will be exercised during force-on-force training exercises at least once every 18 months.

d. A record of the exercise will be maintained for 18 months.

3-8. Coordination and integration of plans

Protection, recapture, recovery, and transportation plans for chemical agent security will be coordinated to assure that protection of chemical agents receive adequate coverage in such plans. The following guidance applies:

a. The tenant or custodial chemical agent organizations will participate in host installation planning. There will be provisions in such plans for mutual support of collocated forces.

b. When feasible, plans will be integrated with those of nearby military installations.

c. When practical, plans will include support agreements with other Service forces to enhance the site security and recovery of chemical agents. Interservice support agreements will be used to ensure continuity of support.

d. The plan will be coordinated with organizations providing security forces support to chemical agent facilities, to include Federal and local civil law enforcement authorities, as applicable.

3-9. Classification of plans

Security and defense plans, including recapture and recovery plans in chapter 12, will be appropriately classified according to the security classification guidance in AR 380-86.

3-10. Physical security plan outline

This outline will be used in the preparation of the site physical security plan. Portions of this outline may not be applicable to a specific location. However, local requirements may direct inclusion of additional material. Care will be taken to mark pertinent portions of the plan as classified information according to AR 380-86.

a. *Classification and authority.*

Cite the overall security classification of the plan and the authority for such classification.

b. *Name and location of the facility.* Self-explanatory.

c. *Mission of the facility.* Self-explanatory.

d. *Purpose.* Cite a brief purpose of the plan. The plan should ensure that good planning has integrated all forces, devices, and equipment into an effective security system.

e. *Objectives.* Cite the objectives of the plan. (For example, protection of the nuclear reactor and SNM from sabotage, theft, loss, diversion, or unauthorized access.)

f. *Threat analysis.* Analyze the threat against chemical agents for sabotage, theft, loss, seizure, or unauthorized access, use, or diversion. Review and consider the postulated threat. Consider the tactics and associated weapons, tools, and explosives that the aggressors are likely to use. Review and evaluate local threat information obtained from intelligence and law enforcement sources. Consider any recent security incidents (related or unrelated to chemical agents) which may have a bearing on the overall threat analysis.

g. *Vulnerabilities.* Review results of site vulnerability assessment. Identify critical and other structures, containers, buildings, and work areas that require protection. Consider their location, size, function, and contents even if they are only used occasionally. Consider the aggressor tactics included in the threat analysis.

h. *Priorities.* Establish priorities for protecting various areas within the chemical agent facility.

i. *Limited and exclusion areas.* Delineate these areas. Include controlled areas.

j. *Equipment and devices to detect or delay intrusion.* Identify equipment and devices to detect or delay intrusion.

(1) *Perimeter boundary.*

(a) *Type.*

- (b) Construction.
- (2) *Clear zones.*
- (a) Widths.
- (b) Surface undulations and ditches.
- (c) Obstacles (for example, poles, trees, boulders, structures, and so forth) that could not be removed.
- (d) Culverts, utility tunnels, and other structures.
- (3) *Gates.*
- (a) Type and construction (personnel, vehicle, or both).
- (b) Locations.
- (c) Hours of operation.
- (d) Locking means and procedures.
- (4) *Signs.*
- (a) Types—no trespassing, persons/vehicles subject to search, use of deadly force, and bilingual when appropriate.
- (b) Location.
- (5) Identify types of inspection or maintenance.
- k. *Security lighting.* Identify the type of lighting utilized and the procedures established.
- (1) Types (area, glare projection, controlled (width of lighted strip), and portable).
- (2) Type of light source (low-pressure sodium vapor, high-pressure sodium vapor, mercury vapor, incandescent).
- (3) Use, control, and standards (foot-candles).
- (a) Perimeter.
- (b) Gates.
- (c) Interior areas and structures.
- (4) Inspections and maintenance.
- (5) Emergency actions for power failure—who does what.
- (6) Emergency generator—type, location, fuel supply, operating instructions, testing procedures, maintenance requirements.
- (7) Emergency backup lighting - operating instructions.
- l. *Protective alarms.* Identify the systems to be utilized and the procedures to be followed.
- (1) Types.
- (2) Locations.
- (3) Procedures for operation, monitoring, and activation or deactivation.
- (4) Tests and anti-tamper procedures.
- (5) Inspections and maintenance.
- (6) Record/logs.
- (7) Actions by security force when alarms occur or when the alarm system, or any part of the system, becomes inoperative.
- (8) Duress system.
- (9) Warnings and alarms.
- (10) Emergency or back-up power sources
- m. *Communications systems.* Identify the procedures to be followed for the communications systems.
- (1) Types.
- (2) Locations.
- (3) Use.
- (4) Tests.
- (5) Inspections and maintenance.
- (6) Records/logs.
- (7) Emergency and/or backup power sources.
- n. *Locks and keys.* Identify the locks and keys to be utilized and the procedures to be followed.
- (1) Types.
- (2) Use.
- (3) Locations.
- (4) Maintenance and rotation.
- (5) Controls, logs, accountability.
- (6) Two-person control keys.
- o. *Delay systems.* Identify the delay systems to be utilized and the procedures to be followed.
- (1) Types.

- (2) Locations.
- (3) Total delay time provided (for example, time needed to gain access to chemical agents).
- (4) Inspections and maintenance.
- p. Security procedures during construction, renovation, or extensive maintenance.* Provide instructions when applicable.
- q. Measures to control personnel vehicles and material.* Determine what restrictions on access and movement are required for each critical area or structure (for example, limited area, exclusion area, material access area, vital area).
 - (1) Personnel access controls.
 - (a) Assigned personnel—PRP and non-PRP.
 - (b) Visitors.
 - (c) Maintenance personnel (Government and contractors).
 - (2) Escort requirements.
 - (3) Search and seizure procedures.
 - (4) Duress system.
 - (5) Nonoperational hours access procedures.
 - (6) Emergency entrance procedures. (Means of immediate entry for fire, security, chemical agent disposal, and medical personnel.)
- r. Personnel identification system.* Personnel recognition and identification cards or badges for assigned personnel, visitors, and maintenance personnel.
 - (1) Identification cards.
 - (2) Badges.
 - (3) Entry control rosters.
- s. Vehicle control.* Identify the delay systems to be utilized and the procedures to be followed.
 - (1) Search and seizure procedures.
 - (2) Parking locations during duty and non-duty hours (include security requirements).
 - (3) Restrictions and control on:
 - (a) Privately-owned vehicles.
 - (b) Government vehicles.
 - (c) Contractor vehicles.
 - (d) Maintenance vehicles.
 - (e) Commercial vehicles.
 - (f) Railroad cars and trains.
 - (g) Emergency vehicles (for example, security, fire, and medical).
 - (4) Registration, if applicable.
- t. Material control.* Identify requirements for controlling material in the area.
 - (1) Incoming.
 - (a) Requirements for admission, to include restrictions.
 - (b) Inspection, search, and seizure.
 - (c) Sealed packages and containers.
 - (2) Outgoing.
 - (a) Documentation required.
 - (b) Inspection, search, and seizure.
 - (3) Classified documents or materials, controls, and procedures for incoming and outgoing, including emergency destruction.
- u. Security forces.* Identify procedures for the security force.
 - (1) Type—military, civilian and contractor (U.S., foreign).
 - (2) Composition and organization.
 - (3) Authority and jurisdiction.
 - (4) Weapons, ammunition, and equipment.
 - (5) Rules of engagement and use of deadly force (Include fixed wing aircraft and helicopter assault).
 - (6) Training.
 - (7) Actions to be taken under adverse weather and limited visibility conditions.
 - (8) Posts.
 - (a) Locations.
 - (b) Areas of responsibility.
 - (c) Hours.

- (d) Duties and functions, including general patrol routes (Vary patrol routes and rotate stationary posts to combat boredom.)
- (e) Reporting procedures.
- (f) Employment of military working dogs (if applicable).
- (9) Response force.
 - (a) Purpose and mission.
 - (b) Size, composition, and organization.
 - (c) Weapons, ammunition, and equipment.
 - (d) Location and call-out procedures.
 - (e) Reaction times.
 - (f) Protection of response vehicles from sabotage.
 - (g) Protected response means and alternate routes.
 - (h) Actions for multiple site intrusions.
 - (i) Training, including frequency of testing.
- (10) Augmentation force.
 - (a) Purpose and mission.
 - (b) Size, composition, and organization.
 - (c) Weapons, ammunition, and equipment.
 - (d) Location and call-out procedures.
 - (e) Response time.
 - (f) Tactical plan (attach as appendix).
- v. *Other supporting security forces.* Identify procedures.
- w. *Emergency actions of general nature.* Actions not covered by this plan which are required for serious emergencies, such as fire, bomb threats, serious injuries, and so forth.
- x. *Chemical agent movements.* Identify procedures.
 - (1) Procedures for movement.
 - (2) Training of security personnel.
- y. *Coordination.* Provide contact names and telephone numbers of agencies with whom this plan was coordinated with.
 - (1) Integration of this plan with installation supporting agencies.
 - (2) Liaison and coordination with nearby military units (including, police, intelligence agencies,) and with civil agencies (including civil police and FBI, as appropriate).
- z. *Appendixes.* Include the following appendixes:
 - (1) DA Implementing Instructions to the DOD Postulated Threat.
 - (2) Local security threat.
 - (3) Vulnerability assessment.
 - (4) Tactical defense plan.
 - (5) Recapture and recovery plan.
 - (6) Guard orders.
 - (7) Entry and exit procedures for Chemical Weapons Treaty Compliance Inspections.
 - (8) DEMIL Facility Security Plan, if applicable.

Chapter 4

Perimeter Security

4-1. Category I and II Chemical agents

The requirements in this chapter are applicable to storage sites containing category I or II chemical agents.

4-2. Perimeter security system

The perimeter security system for the storage areas will provide a positive means of detecting and deterring unauthorized entry to an intruder(s) to enable the security force to execute the appropriate response.

4-3. Perimeter boundary fencing

a. *Concept.* Perimeter fences will clearly delineate and impede entry to the zone of protection associated with limited and exclusion areas. When permanent perimeter fences are not available for any reason, a request for deviation

will be requested and temporary physical barriers, additional sentries, patrols, or other security measures will compensate for their absence.

b. Natural barriers. Natural barriers, such as rough terrain or bodies of water, do not constitute acceptable security protection for limited areas.

c. Building walls. Building walls may be incorporated in the perimeter fencing system provided they are subjected to visual assessment. However, walls of structures storing chemical agents will not be considered as a barrier fulfilling boundary fence requirements.

d. Number of fences. The limited area surrounding chemical agent storage structures will be protected by two perimeter fences. Perimeter fences will be located, with due consideration to required clear zones, terrain features, property lines, and building layouts, not less than 30 feet nor more than 150 feet from buildings or objects being protected.

e. Fence specifications. Fences will meet the standards and specifications described in U.S. Army Corps of Engineers (USACE) Standard Design Drawing (STD) 872-90-04 for nonsensored fence and/or 872-90-05 for sensed fence, and have a seven feet high fabric (FE-7 fence) plus outriggers. Existing fences that do not meet the new fence standards in this regulation may continue to be used (waiver/exception not required) until replacement is necessary at which time the new fence standards will apply. Additional requirements are as follows—

(1) *Vehicle barrier cable.* A steel cable of sufficient strength to impede vehicle penetration should be installed outside the outer fence in which topography permits high speed approach (excluding authorized vehicle entry points).

(2) *Soil-Stabilization.* Ground surfaces will be made stable in areas where the sand, shifting soils, or surface water may cause erosion and thereby assist an intruder in penetrating the perimeter security system. Where surface stabilizing is not possible or practical, concrete curbs or sills, or other similar type anchoring devices, extending below ground level will be used. Sites should perform a risk assessment to determine if erosion may create a security vulnerability by reviewing past fence inspection records and engineering specifications. If the assessment indicates that erosion may create vulnerability and soil stabilization is impractical, then concrete curbs or other anchoring devices, extending below the ground level, should be used.

(3) *Gates.* Perimeter fences will have a minimum number of vehicular and pedestrian gates consistent with operational requirements. Gates will be designed so that traffic through them will be under the positive control of the security force. Except in emergencies and operational necessity, and to support chemical agent DEMIL delivery operations, entry and exit from storage areas will always be made through the main vehicular and pedestrian gates. Gates will be closed and secured when not in use. Semi-active gates will be locked with low-security padlocks (NSN 5340-00-158-3807, with chain, or NSN 5340-00-158-3805, without chain). Gates will be structurally comparable and provide the same resistance to penetration as associated fences. The bottom of the gate will be close enough to firm ground to prevent an intruder from crawling under the gate. Gates will be equipped with appropriate barbed wire toppings (for example, outriggers or vertical arm brackets).

(4) *Drainage openings.* Drainage structures, water passages, and other openings penetrating the perimeter fence will be barred to prevent penetration. Openings to drainage structures having a cross-sectional area greater than 96 square inches and a smallest dimension greater than 6.4 inches will be protected by securely fastened, welded bar grills. As an alternative, drainage structures may be constructed of multiple pipes, each pipe having a diameter of 10 inches or less. Multiple pipes of this diameter also may be placed and secured in the “in-flow” of a drainage culvert to prevent intrusion into the area. Covers to manholes of drainage structures penetrating the perimeter fence will be secured with a low-security padlock (NSN 5340-00-158-3807 or NSN 5340-00-158-3805).

4-4. Clear zones

The purpose of clear zones is to deny protection and concealment to intruders. The following requirements will apply—

a. When a single fence is used, clear zones will extend 30 feet on both sides of the fence.

b. Clear zones will extend 30 feet outside the outer fence, the entire area between the fences, and 30 feet inside the inner fence.

c. Clear zones will be clear of all obstacles, topographical features, and vegetation which could reduce the effectiveness of the perimeter fence (for either ingress or egress), impede assessment, or provide cover and concealment for an intruder. If clear zones are impractical to maintain because of serious continuing erosion problems environmental considerations (for example designated wetlands, and so forth) or other factors, appropriate security measure will be used. Security measures will compensate for clear zone terrain features or obstacles that may provide areas for intruders to hide in, offer intruders protection from security force weapons, or serve as assembly points for attacking forces.

(1) Perimeter light and closed circuit television system (CCTV) camera poles that can potentially aid in circumventing the fences (for either ingress or egress) will be provided with physical barriers to prevent climbing.

(2) Perimeter light poles, fire hydrants, steam pipes, or similar objects, and entry control buildings which are within

the clear zone and represent no aid to counter the purpose of the perimeter fence or preclude assessment do not violate the requirements of a clear zone.

4-5. Security lighting

Security lighting will be provided at chemical agent storage areas to discourage unauthorized entry and to facilitate the detection of intruders approaching or attempting to gain entry into limited and exclusion areas. Security lighting will be used during hours of darkness and reduced visibility. The following requirements will apply—

a. Perimeter lighting.

(1) Perimeter lighting will be positioned and designed to enable the detection of persons in the entire clear zone, inside the inner perimeter fence, between the fences, and outside the outer perimeter fence.

(2) The requirement to light the inner clear zone does not apply where on-call lighting is provided and is activated on demand by site security personnel.

(3) When CCTV is the primary means of perimeter assessment, the lumen output throughout the clear zone may be varied as needed to accommodate the operation of the CCTV or other electronic imaging system. Primary emphasis will focus on detection capability in the outer clear zone and between the fences.

b. Outer clear zone. To facilitate human visual assessment, the outer clear zone, 30 feet outside the outer perimeter fence, will be provided with a minimum of 0.2 foot-candles (2 lux) illumination measured on the horizontal plane or a minimum of 0.4 foot-candles (4 lux) illumination measured on the vertical plane. This measurement will be taken 6 inches above the ground during normal visibility conditions at a point 30 feet from the outer fence.

c. Vehicular and pedestrian gates. Vehicular and pedestrian gate lighting will be of sufficient intensity and designed for personnel identification and detection of unauthorized items. Such gates will be provided with 2.0 foot-candles (20 lux) horizontal illumination during normal visibility conditions, measured 6 inches above ground level.

d. Exterior doors. Security lighting will be provided for exterior doors of chemical agent storage structures. Lights will be of sufficient intensity to allow detection of persons at the exterior doors. Switches for exterior lights will be installed so they are not accessible to unauthorized persons. Exterior lights will be covered with wire mesh screen or vandal resistant lenses to protect the lights from being broken by thrown objects.

e. Restart capability. The site security lighting system will have a restart capability and produce required lumen output within 3 minutes after primary or emergency power is applied. See paragraph 6-3 for standby generator power requirements.

f. Perimeter lighting circuits. Perimeter lighting circuits will be designed so that failure of one or more lights will not affect operation of the remaining lights.

g. Patrol roads. Patrol roads or paths should not be lighted (incidental lighting is acceptable).

h. Lighting fixtures. Whenever possible, lighting fixtures will be positioned to avoid blinding of guards from glare and silhouetting of guards.

i. Control of site security lighting. The site security force will be provided a means of controlling site security lighting. Perimeter lighting controls will be installed in the site security control center (SSCC) or entry control facility (ECF).

j. Turning off site security lights. The site physical security plan may provide for turning off the site security lights to defend the site under anticipated or actual emergency conditions. This includes turning off the lighting over storage structure doors. A sweep will be conducted of the area immediately after restoring the site security lights.

k. Perimeter lighting will not be turned on and off on a random basis during nonemergency.

l. Nonemergency conditions. Perimeter lighting may be turned off during security force exercises; however, appropriate security measures will be taken for the lack of such lighting. In such cases, a sweep will be conducted of the area immediately after restoring the site security lighting.

4-6. Entry control facilities

ECFs will be provided to control the entry and exit of authorized personnel and vehicles. This facility will be part of the perimeter security system, and will be the point from which personnel and vehicle control and badge operations will normally be conducted. The facility will be equipped with lighting to permit personnel and vehicle identification and inspection at night in any weather condition. The basic makeup of the ECF will include a gate house, a personnel entry gate, and a vehicle entry area.

a. ECF gate house. The ECF gate house will be constructed to afford protection to security force personnel from small arms fire. Existing ECFs will be modified to afford this protection. Use of sandbags, concrete, steel plates, or bullet-resistant glass or plastic are means by which this protection may be attained. Additionally, the ECF will constitute a fighting position, from the inside or on top, for security force personnel. Within the ECF will be an area for secure badge control and necessary security force accommodations for assigned personnel. Provisions will be made to enable security personnel under duress to transmit signals discreetly to other security personnel. The ECF may also contain the IDS control center, the SSCC, the perimeter visual-assessment system, and/or the RF. If a chemical agent disposal facility is co-located with the storage chemical limited area, a separate ECF may be constructed to accommodate additional personnel and traffic supporting the disposal mission.

b. Personnel entry area. The personnel entry area will be designed to ensure that personnel entering or exiting the site are under the positive control of security force (for example, by remotely operated gate, door, or turnstile controlled from within the ECF).

c. Vehicle entry area. The vehicle entry area will consist of two gates constructed in such a way that when a vehicle enters, the outer gate is opened while the inner gate remains closed. The outer gate then will be closed behind the vehicle before the inner gate is opened to permit the vehicle to enter. The reverse procedure will be followed for vehicles exiting the area. Both portal gates will be constructed or modified to incorporate a positive locking feature when closed. An electrically operated gate will have a capability to be manually operated in the event of malfunction or other emergencies. Both gates may be opened at the same time for emergencies or operational requirements. When the gates are opened at the same time, appropriate security measures will be taken to ensure that the area is protected against unauthorized entry.

d. Vehicle crash barriers. When appropriate, vehicle crash barriers will be installed at both the inner and outer gates to reinforce the vehicle entry area.

4-7. Perimeter detection and assessment system

Early detection and near real-time assessment are essential for a prompt and effective response by security forces to any attempt to penetrate the site perimeter. A perimeter intrusion detection system (IDS) will be employed to meet this requirement. Paragraph 2-7d (6) provides guidance for compensatory security measures when IDS has not been installed or is not planned for installation.

a. Perimeter IDS. Two continuous lines of IDS sensors with line supervision will be installed to detect unauthorized entry into the limited area along the site perimeter. Each line of sensors will use a different sensing phenomenon.

b. Site survey. An IDS site survey will be conducted according to requirements in AR 190-13.

c. IDS criteria. IDS criteria in paragraph 5-7 apply.

d. Compensatory measures. Appropriate compensatory security measures will be taken immediately upon discovering an inoperable IDS sensor or sensors. At a minimum, two hour checks of the perimeter, on a random basis by security force personnel is required when perimeter IDS is inoperable.

e. Assessment. A means will be provided to assess the cause of all alarms activated at the perimeter security system in near real-time. Near real-time assessment may be satisfied when assessment of the actual cause for activation of the sensor alarm is by either direct visual assessment or electro-optical equipment (imaging system).

f. Imaging systems. Imaging systems provide a remote visual image of activity in an area under surveillance. CCTV, infrared, or radar are techniques that may be used to meet requirements in *e*, above.

g. Protection of monitor station. The primary monitor station used for visual assessment will be located in an area that is protected against small arms fire. CCTV cameras do not require hardening.

4-8. Restricted area designation

a. Commanders of military installations and facilities have the authority to publish and enforce regulations for safeguarding personnel, facilities and property. This authority is derived from the Internal Security Act of 1950 (50 United States Code (U.S.C.) 797), and is implemented by DODD 5200.8 and DOD 5200.8-R.

b. The garrison commander will designate biological select agent and toxins (BSAT) facilities as restricted areas.

c. Post signs or notices in conspicuous and appropriate places to identify a restricted area (except when such action would tend to advertise an otherwise concealed area, or when in conflict with Host Nation Agreements). Position signs so not to provide concealment of an intruder or obstruct visual assessment.

d. Signs will read THIS ACTIVITY HAS BEEN DECLARED A RESTRICTED AREA BY AUTHORITY OF THE OF THE INSTALLATION COMMANDER IN ACCORDANCE WITH THE PROVISIONS OF THE DIRECTIVE ISSUED BY THE SECRETARY OF DEFENSE ON 24 April 1991, PUSUANT TO THE PROVISIONS OF SECTION 21, INTERNAL SECURITY ACT OF 1950. UNAUTHORIZED ENTRY IS PROHIBITED. ALL PERSONS AND VEHICLES ENTERING HEREIN ARE LIABLE TO SEARCH. PHOTOGRAPHY OF THE FACILITIES IS PROHIBITED WITHOUT SPECIFIC AUTHORIZATION FROM THE COMMANDER. DEADLY FORCE IS AUTHORIZED.

e. Existing signs containing essentially the same wording as in USACE (United States Army Corps of Engineers) Drawing 872-90-01 may continue to be used until replacement is necessary at which time the required wording in USACE Drawing 872-90-01 will be used.

4-9. Perimeter defensive positions

a. Requirement for defensive positions. The configuration of each storage area, coupled with the capability of security force personnel to react to attempted penetration in a protected mode, will dictate the requirement for perimeter defensive positions.

b. Location. Storage area commanders will determine the need and location of perimeter defensive positions based on the results of the vulnerability assessment. If the defensive positions are not needed, this determination will be included in the site vulnerability assessment.

c. Fighting positions. Perimeter defensive positions may be constructed as prepared fighting positions when deemed necessary by the local commander. Prepared fighting positions should provide clear fields of fire and provide protection against small arms fire.

d. Flexible response. Care must be taken to ensure site planning is not limited to fixed perimeter defensive positions. The objective of site defensive planning is to provide a flexible response, using sound tactics to defeat an intruder.

4-10. Vehicle barriers

a. Terrain considerations. Terrain features surrounding the storage area perimeter may provide suitable approaches for wheeled vehicles to gain access by ramming the fences or entry gates. In such cases, commanders concerned will provide appropriate barriers to counter the high speed vehicular threat.

b. Examples of barriers. The following are examples of barriers that may be used—

- (1) Road speed bumps and gate crash bars.
- (2) Railway rails or angled and vertical steel posts filled with concrete partially embedded below the ground.
- (3) Concrete highway median barriers and concrete blocks.
- (4) Sand or concrete filled 55-gallon drums.
- (5) Log barriers, excavations, and ditches.

c. USACE drawings. USACE Drawing 872-50-01 depicts various barriers for use at installation access points. Some of these barriers may be useful at chemical agent storage area entrances.

4-11. Security during construction projects

When substantial construction is underway at the storage site, the construction area will be physically separated from the area containing chemical agents. This will be accomplished by barriers to impede and delineate entry to the zone of protection associated with the area containing chemical agents. Added security measures will be taken to detect and prevent entry into the area containing chemical agents. Physical boundaries do not need to be hardened; the intent is to segregate the construction zone from areas containing chemical agents. Uncleared personnel will be kept under continuous escort at all times by individuals allowed unescorted access to the chemical limited area.

4-12. Limited area topography

a. Vegetation. Underbrush and low hanging tree branches within the limited area which could be used to obstruct security force observation, or help to conceal intruders will be removed. Ground vegetation, such as grass, may be retained; however, it will be kept trimmed to permit efficient use of wide area detection, tracking and surveillance system and preclude easy concealment of intruders. The following guidance applies:

- (1) The situation prevailing at each chemical storage site will be treated on a case-by-case basis.
- (2) At individual sites where removal of vegetation within the limited area is cost prohibitive, or could result in a downwind chemical safety hazard to nearby civilian populations, a detailed analysis of the vulnerabilities (chap 16) associated with the topography will be conducted and a judgment rendered by the commander as to the acceptability of existing conditions. The commander's decision on conclusions and recommendations will be documented in the site vulnerability assessment.

b. Terrain. Ravines, gullies, sink holes and other depressions not necessary for drainage or erosion control and which provide a tactical advantage to intruders will be filled in or have obstacles emplaced to impede quick movement. Depressions that provide tactical advantage to the security force need not be filled in or protected with obstacles.

Chapter 5 Storage Requirements

5-1. Category I or II chemical agents

The provisions of this chapter apply to category I or II chemical agents.

5-2. Bulk storage

Category I or II chemical agents will be stored as follows, unless otherwise specified in this regulation—

a. Standard storage structures. Acceptable storage structures are those Army igloos, Navy arch-type magazines, and earth-covered, corrugated steel, arch-type magazines listed in DOD 6055.9-Std as supplemented by AR 385-64.

b. Nonstandard storage structures.

- (1) *Walls.* Walls will be constructed of either of the following:
 - (a) Eight-inch thick concrete, reinforced with number 4 reinforcing bars at 9-inch centers in each direction and staggered in each face to form a grid approximately 4½-inches square.
 - (b) Eight-inch thick concrete block laid with cores in line (number 4 bars threaded through cavities) and then filled

with mortar, reinforced with a 3-inch lining of fibrous concrete bonded to the block by 2½-inch case-hardened nails on 6-inch spacing and driven 1 inch into the block prior to casting the liner.

(2) *Ceilings and roofs.* Ceilings and roofs will be designed to suit the structural requirements of the spans between the supports to meet required safety criteria. Sufficient concrete and reinforcing steel will be included to offer resistance to penetration equal to that provided by the walls.

(3) *Floors.* Floors will be of reinforced concrete construction. Where the floor slab acts as the ceiling of an underlying room or area, it will be at least equivalent to the criterion specified in (2), above.

(4) *Doors.* Doors, as a minimum, will be constructed of 1¾-inch thick wood with 12-gauge hardened steel plate on the outside or be of standard 1¾-inch thick, hollow metal, industrial-type construction with minimum 14-gauge skin plate thickness, internally reinforced vertically with continuous steel stiffeners spaced 6 inches maximum on center. Door bucks, frames, and keepers will be rigidly anchored and provided with anti-spread space filler reinforcements to prevent disengagement of the lock bolt by prying or jacking of the door frame. Construction requirements for door frames and thresholds should be as exacting as those for the doors themselves. For example, where metal doors are used, the frame and threshold also will be metal.

(5) *Door hinges.* Various types of hinges are commercially available. For secure area doors—

(a) The hinge will be of sufficient strength to withstand the rigors of constant use and the unusual weight of the doors.

(b) Hinges, when mounted, will be concealed by the door structure or otherwise protected from outside tampering when the door is closed.

(c) If the door and door frame are ordered as a unit, as in the case of some hollow metal or industrial grade steel doors, the manufacturer will be required to provide hinges and hinge pins which cannot be removed or, if removed, will not provide access when the door is locked.

(6) *Unsecured door hinges.* Unsecured hinges on doors of existing structures will be secured to prevent removal by any of the following means—

(a) Brazing, welding, or riveting the hinge pins.

(b) Installing fixed pin security hinges.

(c) Modifying the hinge side of the door by incorporating a tongue-in-groove so that when the door is fully closed and the locking mechanism engaged, the tongue is seated in the groove and the door cannot be removed from the frame even with the hinges removed.

(7) *Windows and openings.* Windows and openings (less entrances) in structures in which chemical agents are stored will be provided with physical barriers such as grillwork or screening that have a level of resistance to forced entry that is at least equivalent to the surrounding walls.

(a) Movable windows and opening covers will be provided with locking devices that are not readily visible or accessible from the outside.

(b) All windows and openings (such as vents, ducts, and conduits) on the walls, floors, and ceilings having an area greater than 96 square inches with a smallest dimension greater than 6 inches will be protected by a rod and bar grill which, at a minimum, is constructed of 1¼-inch by 3/8-inch horizontal flat steel bars at 8 inches maximum center to center, with 3/4-inch vertical steel rods a maximum of 12 inches center to center welded or woven through the 1¼-inch surface of the flat bars.

5-3. Locking systems

a. *Access doors.* Doors used for main access to chemical agent storage structures (for example, magazines, igloos, and buildings) containing chemical agents will be locked with the Internal Locking Device, approved for use on structures protecting chemical and nuclear weapons (*see* <http://locks.nfesc.navy.mil/ILDIntro.htm>) or two high-security padlocks (MIL-DTL-43607), NSN (national stock number) 5340-00-799-8248, NSN 5340-01-217-5068, or NSN 5340-00-188-1560. Each high-security padlock will be mounted on a high-security shrouded hasp (MIL-DTL-29181C), NSN 5340-01-196-2547 (right hand), or NSN 5340-01-235-6907 (left hand).

b. *Other doors.* Doors (para 5-2 b(4)) which are not ordinarily used for access will be secured from within and will provide resistance to penetration equivalent to that of the structure itself. The following requirements apply:

(1) Doors will be secured by a substantial locking bar or dead bolt from inside the structure.

(2) Doors that cannot be secured from the inside with locking bars or dead bolts will be locked with low-security padlocks that are mounted on steel hasps that provide protection equal to the lock.

(3) Panic hardware, when required, will be installed so as to prevent opening the door by fish-wire operation of the bolt from outside the door.

c. *Perimeter gates.* Perimeter gates, vents, grills and gratings will be locked with low-security padlocks, as in (2), above. Hasps that are mounted on gates, vents, grills, and gratings will provide protection from forced entry equal to the lock.

d. *Existing locking bars.* When high-security shrouded hasps are installed on storage magazines or igloos, any

existing locking bars and T-pins should be left in place to aid in opening and closing doors and prevent any future misalignment of such hasps (that is, due to settling of doors or damage to hasps).

e. Key and lock control. Key and lock controls will be established according to requirements in chapter 8.

5-4. Storage structure entry hindrance

Whenever feasible, a King-Tut block will be placed in front of bulk storage structure access doors to serve as an additional obstacle to unauthorized entry and exit. If King-Tut blocks are not available, a cement block of sufficient weight requiring handling equipment for its movement will be used.

5-5. Security construction verification

a. Qualified engineering personnel will verify the construction composition (for example, walls, ceilings, roofs, floors) of storage magazines, and igloos, used for the storage of chemical agents.

b. The construction verification statement will be in writing and will be signed and dated by the responsible engineer official. The statement will indicate whether or not the storage structure conforms to the construction criteria of the applicable regulation that is in effect on the date of the verification.

c. The statement will specify the date of this regulation and state that the construction criteria meets the storage requirements for the category of chemical agents involved. (Any deviations from the construction criteria will be noted for waiver and exception procedures).

d. The statement will be posted inside each storage structure. A blanket statement may be issued at an installation for all storage structures that are constructed according to the same construction criteria. Under these circumstances a copy of the blanket statement need not be posted in each storage structure, but the statement will be readily available for inspection. A blanket statement will identify the location and number of each storage structure, and contain the information in *c*, above.

e. Construction verification statements apply to existing structures, new construction, and modifications. Construction verification will be revalidated by qualified engineering personnel at least every 5 years. When construction modifications are made, a new construction verification statement is required.

f. Construction verification statements will be reviewed during physical security inspections.

g. DA Form 4604-R (Security Construction Statement) may be used for this purpose. A reproducible copy of this form is located in AR 190-11.

5-6. Binary precursors

a. Designation as chemical agents. Binary components will be secured and controlled as chemical agents when—

(1) Binary munitions with both the critical and noncritical binary components are uploaded.

(2) Binary components are mixed to produce chemical agents for research, development, test, and evaluation (RDTE) operations; quality assurance testing of nuclear, biological, and clothing and equipment; or chemical agent training.

(3) Both critical and noncritical binary components are present in the same storage structure or laboratory room.

b. Storage of critical binary components. Critical binary components not designated as chemical agents will be stored according to security requirements in AR 190-11.

5-7. Interior and exterior IDS requirements

a. Installation of interior IDS. All storage structures, buildings, or rooms in which chemical agents are stored will be protected with interior IDS to detect the physical opening of any entry way. See AR 190-13 for IDS standards and procurement procedures. The IDS protection will consist of a balanced magnetic switch or other type of sensor capable of detecting intrusions at the opening. Sensors will be installed at all movable openings, doors, windows, and hatches which exceed 96 square inches, with the smallest dimension greater than 6 inches. Sensors will be located inside the structure being protected. IDS control units will be fitted with tamper detection devices and located inside the structure. If the control unit cannot be placed inside the structure, it will be placed in a locked, tamper alarmed, weather-proof, container on the outside of the structure in close proximity to the entrance.

b. Alarm reporting systems. Interior and exterior IDS will consist of sensors integrated by data transmission links into a monitor console. The monitor console will include an audio and visual indicator display terminal, and a map or video display terminal.

c. Secure status. IDS for structures containing chemical agents will be in secure status (active) at all times except when the structure is opened for authorized access. Perimeter IDS will be in a secure mode (active) at all times except when IDS maintenance or repairs are ongoing in the zone of detection. Sensors covering personnel and vehicle portals and entrapment areas may be placed in the access mode (inactive) during shift changes and other high activity periods, provided the zones are observed by an entry controller or CCTV monitored by an entry controller, or other assessment methods.

d. Compensatory measures. If the facility is not protected by an operative IDS, at a minimum, inoperable interior (structure) and exterior (perimeter) IDS will be physically checked by security personnel on a random basis not to

exceed two hour intervals. Appropriate compensatory security measures will be taken immediately upon discovering an inoperable IDS sensor or sensors.

e. Alarm display. Alarm activations for interior and exterior IDS sensors will be displayed at the alarm center. The following provisions will be included—

(1) Audio and visual indicators of alarm status will be displayed on a map or video display terminal. The display selected will graphically present the site configuration as well as the zones being monitored. For existing systems, an audible alarm that identifies the zone in alarm and a camera system that may be used to observe the alarming zone in lieu of a map or video display as long as the system provides near real-time assessment and observation of the zone in alarm.

(2) Audio and visual indications will show line supervision status.

(3) Audio and visual indications will show access/secure status.

f. Backup battery power supply. Backup battery power supply, independent of primary and standby power sources, will be capable of operating the IDS equipment for 4 hours (see para 6–3c).

g. Alarm assessment equipment. Alarm assessment, either visually or through the use of electro-optical (imaging equipment) or other electronic devices will be used to assess exterior perimeter alarms.

h. Radio frequency link. The use of a radio frequency link is permitted when the size of the area would make the cost of hard-wire prohibitive.

i. Data transmission link. The data transmission link will include—

(1) Line supervision to detect and signal attempts of cutting, shorting, splicing, or substituting the transmission link. Such supervision must initiate an alarm when a variance of five percent in the normal line supervision parameter is detected.

(2) All boxes (that is, junction boxes, field distribution boxes, and cable terminal boxes and cabinets) which group interior or exterior IDS sensor inputs, and which are not within structures or zones protected by IDS will be locked and tamper alarmed.

j. Commercial IDS. Follow procedures in AR 190–13.

k. Record of alarms and IDS and sensor failures.

(1) Commanders will ensure that persons monitoring IDS maintain records of alarms and IDS and sensor failures. These records will be used to evaluate IDS effectiveness (reliability, sensitivity, required adjustments or maintenance, and other data intended to maintain or increase security). Records will be retained for 12 months.

(2) Records will include the nature of the alarm, the date and time the alarm was received, the location, and action taken in response to the alarm or IDS and sensor failures.

(3) Supervisors will review records to ensure proper actions were taken, and to identify and correct IDS reliability problems.

(4) Security supervisors will ensure system malfunctions are reported promptly to IDS maintenance personnel for corrective action.

(5) DA Form 4930–R (Alarm Intrusion Detection Record) may be used to record alarms received and IDS and sensor failures.

(6) DA Form 4930–R may be reproduced locally on 8½ X 11-inch paper. A computer-generated printout of alarms may also be used as a substitute, provided all required information has been included.

l. Testing requirements.

(1) The purpose of testing IDS is to ensure reliability of the system and to preclude undetected tampering and neutralization of the system.

(2) Newly installed interior (structure) and exterior (perimeter) IDS will be tested and certified operational prior to being placed in service and tested periodically thereafter. The goal of testing sensors initially and periodically is to ensure an intruder will trigger an alarm when he or she comes within range of a particular sensor.

(3) Performance tests of existing and newly installed interior and exterior IDS will be conducted while monitoring the alarm panel for the presence of alarm conditions. Tests of exterior IDS will be evaluated for uniformity along the entire length of the site perimeter.

(a) Performance tests consist of testing all installed sensor devices to ensure the complete system complies with regulatory requirements. Discovery of failures will require additional tests once repaired.

(b) Endurance test consists of a 30 consecutive day period following an evaluation that the sensors have been properly installed and is operational

(c) The maximum nuisance and false alarm rates (NAR/FAR) will be established using the manufacturer's specifications operating environment. The maximum NAR and FAR will be approved by the contracting officer or his/her designated representative.

(4) In those instances where sensors are installed in such a manner as to preclude individual testing, the sensors may be tested as a group.

(5) IDS technical manuals and operating instructions for installed IDS will be available for reference to ensure

sensitivity setting criteria and testing methods are properly applied. When the manuals and operating instructions are not available for any reason, supporting engineer personnel will be contacted for technical assistance and advice.

m. Testing of interior sensors. Sensors installed on entrances to storage structures, buildings, or rooms, will be tested by causing an actual alarm at least quarterly, unless technical specifications require more frequent testing.

(1) Depending on the type of sensor involved, the alarm activation will include opening doors, or deliberate movement within the structure (when alarmed in this configuration).

(2) Physical entry into the chemical storage structure is not required to test the door sensors. Opening the door slightly to cause an alarm is sufficient (the alarm must activate prior to achieving the capability to physically access the door sensors).

(3) Doors that are opened during the quarterly period for any reason may be counted in the quarterly testing requirement. Security must be present during these tests to ensure local testing procedures are being followed.

(4) Written instructions will be provided for testing interior sensors.

(5) Testing will be accomplished by security personnel, or by IDS maintenance personnel or operational personnel under the supervision of and in the presence of security personnel.

(6) Where advanced sensor systems which provide the capability to remotely stimulate individual sensors via an electronically activated sensor phenomenology device are installed, this capability may be used to fulfill the testing requirement.

(7) The quarterly testing requirements may be modified for sensors that are located inside secured, pressurized toxic processing areas of chemical demilitarization facilities (chap 15), to mitigate health and safety concerns. These sensors may be tested at appropriate specified frequencies as determined by operational health and safety requirements. The justification for changing the quarterly testing requirement for such sensors will be documented and included in the facility security plan.

n. Testing of exterior sensors. Randomly selected sections or zones of the perimeter exterior IDS will be tested by causing an actual alarm and in such a manner that the entire perimeter is tested at least quarterly. The testing will be accomplished by security personnel or by IDS maintenance personnel under the supervision of and in the presence of security personnel.

(1) Site specific written test procedures will be prepared to ensure the sensitivity and reliability of sensors with respect to the intrusion modes an intruder could reasonably be expected to use. The reasonable intrusion modes include vehicle crossing and humans running, jumping, walking, or crawling through or over the detection zone. Sensor sensitivity adjustment standards will consider intruders with different types of physical characteristics (weight and height), and the speed and duration of penetration.

(2) Testing of sensors installed on fences will be conducted in a nondestructive manner. Testing methods that may potentially damage the sensors or supporting structures, such as climbing on or cutting the chain link fence fabric will not be used. The manufacturer's recommended testing procedures, when available, will be used to verify sensor sensitivity. When such manufacturers test procedures are not available, MACOM or locally developed and approved procedures will be used. In any case, the testing procedures selected must activate the fence protective sensors and cause an alarm in response to the reasonable intrusion modes.

o. Sensor equipment testing. Exterior and structure sensor equipment tamper devices securing enclosures or cabinets which themselves are protected by other adjacent sensor equipment will be tested at least quarterly, unless technical specifications require more frequent testing.

p. Record of tests. A record of all sensor tests will be maintained for 12 months. The record will reflect the date of the test, the name of person conducting the test, results of the test, and any required corrective action resulting from the test.

q. Maintenance. Routine system maintenance will be conducted in accordance with the manufacturer's recommendations. Documentation will be available to validate the manufacturer's recommended maintenance program. Maintenance personnel must be knowledgeable to repair or replace worn or failing components, and to detect evidence or possible indications of tampering with the IDS in accordance with the manufacturer specifications. Security personnel will conduct actual test of IDS of the affected area immediately following maintenance, repair, or modification of IDS, particularly sensors, wiring, circuits, control units, and alarm status indicators. The tests will be documented and recorded in the IDS operator log or automated IDS printout. The tests will be recorded in the guard log.

r. Record of maintenance. A record of IDS maintenance, repairs, and replacement of component parts will be maintained for 12 months. The record may be maintained on DA Form 2404 (Equipment Inspection and Maintenance Worksheet), according to instructions in DA Pam 738-750.

s. Test of IDS backup batteries. A test will be made every 6 months of the IDS backup batteries (to include both interior and exterior IDS) in conjunction with routine system maintenance. The test of backup batteries will require that the batteries assume the full load to ensure that capability exists to support the sensor complement. Voltage and amperage checks are in addition to system loading. Additionally, a test of backup batteries will be made following access by maintenance personnel to battery power sources. Specific testing criteria will be obtained from pertinent IDS technical maintenance instructions. In testing the IDS backup batteries, there is no requirement to go to each storage

structure to test the individual sensors. All backup battery tests will be recorded in the guard log (IDS operator log or automated IDS printout).

Chapter 6

Support Facilities

6-1. Category I or II chemical agents

The provisions of this chapter are applicable to category I or II chemical agent storage facilities.

6-2. Site Security Control Center

Each facility where category I or II chemical agents are stored or handled will have a Site Security Control Center (SSCC). The purpose of the SSCC is to provide a facility from which to provide overall control of security and response force personnel. A separate SSCC is not required when an adequate facility exists and can serve the purpose of a combined SSCC. For example, a separate SSCC is not required for demilitarization facilities. The SSCC will be located centrally within the limited area of the chemical storage site. The SSCC will include the site alarm center, security personnel and vehicle alert facilities. SSCC facilities housing the guard force, communications, and alarm monitors will be protected against small arms fire, unauthorized access, or other hazards that could prevent timely alert in times of emergencies. The facilities will also facilitate effective deployment of security response forces. The SSCC will include provisions for the security force to employ effective fire from within the structure. Facilities to be manned permanently by security forces will be constructed or modified to prevent exposure to adverse weather, including extreme temperatures.

6-3. Power sources

a. Primary electric power. Primary electric power will have sufficient capacity to carry the connected load with the least voltage fluctuation.

b. Standby generator power.

(1) In addition to the primary electric power, all sites will have standby generator power. Standby generator power will—

(a) Be adequate to provide electricity for on-site security and communications functions.

(b) Have an automatic or remote start capability, and be able to assume the full essential on-site load within 60 seconds of a primary power interruption.

(2) The standby generator—

(a) Will be tested monthly under full load to ensure it will be operable when needed. Testing standards, maintenance, and operating log requirements will be followed based on the manufacturer's specifications. Operating instructions will be available for use near the generator.

(b) Transformers, junction boxes, and fuel tanks, will be protected against small arms fire.

(3) When practical, the line distribution grid, which transmits the emergency power within the limited area, will be underground.

c. Backup battery power.

(1) *Automatic switchover.* In case of failure of the alternating current (AC) power, sensor, alarm, and communications systems will be automatically switched over to battery power. Audible and visual indications that AC power has failed or has been restored must be provided.

(2) *Capability of the battery charging system.* Batteries must be capable of operating sensors, alarm, and communications systems for at least 4 hours at the lowest average minimum temperature experienced at the site (cold temperatures affect battery performance). This requirement does not apply to perimeter lighting and CCTV systems. The battery charging system, using AC power, must fully charge the batteries from “no charge” to “fully charged” within 12 hours. After the batteries are charged, the batteries must remain fully charged using the AC power.

(3) *Power supply locations.* The battery power supply may be at one central point or may be located by system component grouping. When each system component has its own battery power source, an audible and visual indication of a loss of AC power must be provided for each component. In either case, the batteries and AC power charger system will be located within the limited area and will be kept under continual surveillance, or contained in an alarmed cabinet to protect the system against tampering.

6-4. Communications

a. Site security communications equipment. Chemical agent facilities will be equipped with a communications system for site security besides the normal administrative telephone system. Underground systems are preferred.

b. Multiple types of communications equipment. Security forces protecting chemical agents will be equipped with multiple types of dedicated and reliable communication equipment. These systems will ensure rapid contact between

security force personnel at the site, the communications control center, and other security forces. The following criteria will be met:

(1) At least two independent systems of communication will be provided between the storage site and the location that will notify security forces. One of these systems will be radio. Each system will have an independent or standby emergency power source.

(2) At least two systems of communication will be provided within the storage site.

(a) A multi-channel two-way radio system capable of linking the SSCC with all patrols and security posts.

(b) The sentry telephone network will connect each permanent sentry post or fixed security post at the SSCC. Terms permanent sentry post and fixed security post are synonymous. Either of these terms refers to a stationary guard post which is occupied on a routine basis at times designated by security force plans/orders or competent authority. The sentry telephone central station will have a capability to call any or all telephones located in fixed sentry locations, separately or simultaneously.

(3) A capability will be afforded for SSCC personnel to communicate with any and all storage structures when they are occupied or open.

(4) Two-way radio communication will be provided between all patrols and the SSCC. Patrols include foot, mobile, and other site security force vehicles.

(5) All radios will have a multiple channel capability.

c. *Guard override capability.* Guard force communications systems may be integrated with fire or other emergency systems. If so, the guard force will be assigned either a priority or an override capability.

d. *Voice radios.* Voice systems procured after 24 March 1989 will be secured or securable by an approved cryptosystem. (See AR 25-2.)

6-5. Maintenance requirements

a. *Continual maintenance.* Structures and equipment located or used at sites will be maintained in a manner that prevents any degradation of safety or security.

b. *Priority maintenance.* Priority maintenance will be given to barrier systems, vegetation control, security lights, clear zones, alarm systems, communications systems, auxiliary power systems, locking devices, gates, storage structures, and security force vehicles, weapons, and equipment.

c. *Daily checks by security.* On-duty supervisors or designated security patrol personnel will visually check all perimeter barriers and clear zones at least once a day during daylight hours. Perimeter lighting will also be checked daily when perimeter lights are turned on at dusk or during reduced visibility. Compensatory security measures will be implemented for any security deviations that cannot be corrected immediately.

Chapter 7 Security Procedures

7-1. Category I or II chemical agents

The provisions of this chapter are applicable to category I or II chemical agents.

7-2. Entry controls

a. *General.* Only authorized personnel will be permitted entry into limited and exclusion areas. Control procedures will assure positive identification of all personnel prior to entry. Identification may be written or by personal recognition. A government issued identification card containing a photograph and sufficient identification data will be used to satisfy the Entry Control Roster (ECR) identification requirement. The following systems and procedures will be incorporated in the entry control program for chemical agent storage facilities:

(1) A security badge system.

(2) Visitor control system.

(3) A duress system.

(4) Package and vehicle inspection system.

b. *Entry criteria.*

(1) *Limited area access.* Responsible commanders, or their designated in writing representative, may permit unescorted entry into limited areas to personnel who have a need for access and who have, as a minimum, an entrance national agency check (ENTNAC), a national agency check (NAC), or national agency check with written inquiries (NACI). Periodic reinvestigation policy established by HQDA (DAMI-CIS) will apply in such cases. Chemical Personnel Reliability Program (PRP) certification is not required. Persons without unescorted access authority must have a need for access, and will be escorted by personnel authorized unescorted access into the limited area.

(2) *Exclusion area access.* Only chemical PRP-certified personnel will be granted unescorted access to exclusion

areas under the two-person rule. Nonchemical PRP personnel must have a need for access and will be escorted by chemical PRP-certified escorts.

(3) *Procedures.*

(a) The responsible commander will establish a system for controlling entry and circulation of authorized personnel and vehicles within the limited and exclusion areas.

(b) Persons requiring escort will be kept under continual control and surveillance.

(c) A system will be established by which personnel who control access into, or escort visitors into a limited or exclusion area can covertly communicate a situation of duress to other operating or security personnel. The duress code will be changed as often as needed to assure integrity or when compromise is suspected. The duress code will also be changed when an individual who was allowed access to the code is no longer authorized access to the code. The security classification of duress codes is prescribed in AR 380–86.

(d) Except as a temporary expedient for convoys and other special circumstances, entry and exit from a limited area will be at a single point and by one person or driver and vehicle at a time. See paragraph 7–7, below, for special control requirements for Chemical Weapons Treaty Compliance Inspections. If chemical agent disposal operations are co-located within the chemical limited area, personnel involved in the chemical disposal operation may process in and out of the area through separate ECFs.

(e) Prescribed entry and exit control procedures may be modified to facilitate rapid entry and exit of personnel and vehicles during the response to an actual emergency (for example, security or medical) and related training exercises. In any event, the safety and security of chemical agents will not be jeopardized. Security measures will be implemented to compensate for the modification of normal entry and exit procedures. Personnel evacuated from the site under rapid exit procedures will be accounted for. As a minimum, rapid entry procedures will provide for verification of authenticity of the emergency force senior member; verification by the senior member of authenticity of emergency forces and numbers involved (opportunity to indicate duress will be provided); and enforcement of the two-person rule when entry to exclusion areas or access to chemical agents is required. When the emergency situation or exercise is concluded, each person admitted under rapid entry procedures will be positively identified at the entry control point before exiting from the area.

(f) Personnel controlling access to the limited area must be able to determine promptly and accurately the number and identity of personnel within the limited area at any given time. Maintaining a running count of personnel may be accomplished by use of a commercial locally made or automated counting device. Automated personnel counts that are part of an approved EACS may be used to meet this requirement. A back up system will be developed in case of system failure.

(g) Security posts and patrols will be notified whenever personnel enter and exit the limited area during non-duty hours; activities are being conducted within their areas of responsibility (for example, within the limited area, open igloo doors, movement of chemical agents, construction efforts, security response exercises, visitors, and so forth); rapid entry and exit procedures are in effect and when unauthorized access or other potential compromise situations occur.

c. *Security identification badges.*

(1) A controlled security badge system will be established for entry into limited and exclusion areas. A badge exchange system may be used. Written detailed procedures will be established to ensure control, accountability, and storage of such badges. Requirements in AR 190–13, AR 600–8–14, and this regulation apply. Cards and badges using mechanical, electronic, or other technological readers to determine access authorization, approved under the provisions of AR 190–13, will ensure system integrity to preclude compromise of the badge system. EACS will be configured in such a way to ensure system integrity and preclude compromise of electric access data. The EACS will operate on a closed computer network specifically designed and established for EACS. Data input to the system will require the badge custodian to have log on and password privileges. Log on and password privileges will be strictly controlled. A process will be developed and reflected in guard orders that allow continuation of access control during partial or complete system failure.

(2) A controlled picture badge system will be provided for personnel authorized access to the limited area without escort. Visitor badges are not required to contain a photograph, however, such badges will be marked to indicate the area for which the badges are valid and if an escort is or is not required.

(a) The picture badges will be distinctively marked to show the status of individuals with respect to the level of access authorized (that is, exclusion area, limited area only).

(b) When a picture badge exchange system is in use and the badge contains sufficient information to assure positive identification of the bearer, the badge may be used in lieu of an entry authorization roster. In such cases, a current, validated list of the badges will be maintained at the limited area entry and exit control point.

(c) If EACS is used in lieu of an exchange badge system, a valid entry control roster is still required. This roster may be maintained electronically if supported by the system.

(3) The badge system for a particular site will be replaced when events or circumstances indicate to the responsible commander the possibility of compromise of the badge system. Other badge replacement requirements in AR 190–13 will also apply.

(4) Badges that are part of an EACS will have their appearance redesigned every three years or when 5 percent are unaccounted for. EACS systems will incorporate the use of a proximity technology or Personal Identification Number (PIN), in conjunction with a biometric feature. Badges will be worn on the outside garment and displayed only when inside the limited or exclusion areas. Exit from the areas will require surrender of the badge at the entry control point of issue if a badge exchange system is used. The only exception is personnel transporting chemical agents to the DEMIL Facility between two separate chemical limited areas.

(5) Badges will have distinctive markings which can be easily recognized by authorized individuals observing the badges.

(6) Badge racks or badge containers will be positioned in the entry control point to ensure the badges are accessible only to individuals assigned to control them. A current list of badges will be maintained. Badges will be inventoried quarterly by serial number and badges maintained at the ECF will be inventoried by count at each shift change.

(7) A badge custodian will be appointed in writing to control the receipt, issue, turn-in, recovery, expiration, and destruction of controlled badges. Written detailed procedures will be established for control, accountability, and storage of such badges. The custodian's duties will include inventory and accountability of the badge system and investigation of stolen, lost, or unaccounted for badges. To preserve the integrity of the badge system, the following will apply:

(a) An accurate written record or log will be maintained to ensure a documented audit trail from receipt or fabrication of badge blank forms at the installation to receipt and disposition of badges by the badge custodian. Shipping or receipt documents will be retained until the badge system is changed. All badges received or fabricated will be listed by serial number. Computer generated badge systems and systems in which badge records or logs are maintained will be configured to maintain system integrity to preclude compromise of the badging system. The record will reflect the serial number of badges on hand, the serial number of badges issued and to whom issued, the disposition of badges turned in, and the serial number of badges that have been lost, stolen, or invalidated. Individuals receiving the badge must receipt for the badge by written signature. In the case of an EACS, a digitally captured signature will suffice.

(b) An unannounced inspection and inventory of records, logs, and all badges will be accomplished every 90 days to ensure integrity of the badge system. Inventory will include badges in sealed packages which will be opened for inspection and inventory. The inspection and inventory will be accomplished by a commissioned officer, Department of the Army civilian, in the grade of GS-7 or higher, or a designated contractor employee. The person appointed to conduct the inspection and inventory must not have a vested interest in the outcome of the inspection and inventory. The inspections and inventories will be reported in writing to the badge custodian. Inspection and inventory discrepancies will be resolved and reported to the commander concerned. The same inspecting/inventory official will not conduct two consecutive inspections/inventories. Badge inspection and inventory results will be recorded and kept on file for 12 months.

(c) Immediate notice will be made of lost, stolen, or invalidated badges. A current list of such badges will be conspicuously posted at entry control points.

(d) Invalidated badges will be destroyed promptly if the persons to whom they were issued are transferred or permanently removed from the chemical PRP, or for other reasons as determined by the commander. EACS that utilize reusable badges will require the badge to be electronically invalidated immediately by the badge custodian when turned in. A feature will be present in the system that allows immediate, remote invalidation of badges in order to limit access by personnel who no longer require it. The custodian will maintain accountability of the badges at all times.

(8) Personnel escorting shipments of chemical agents to the chemical agent disposal facility between two separate limited areas may wear the same badge throughout the day provided the following security measures are in place:

(a) These badges will be strictly controlled at all time and not taken off the installation.

(b) The badges will be distinctively marked to allow access to both chemical limited areas.

(c) Personnel will return their badges to the issuing entry control facility when delivery operations have concluded for the day.

d. Entry control rosters.

(1) The responsible commander/director (or an appointed representative) will prepare and validate the entry control rosters (ECR). The commander/director will appoint the designated representative in writing.

(2) ECRs will contain the name and identification document number of all non-picture badge personnel. The responsible commander or designated representative will sign all ECRs and changes thereto. ECRs and changes will include an expiration date to ensure they are current. The ECRs may be electronically generated as long as the authorized person, as mentioned above, uses Personal Key Information (PKI), encryption software or another form of digital signature to validate the ECR. If system failure dictates the use of manual processing, the other provisions of this regulation will apply.

(3) Individual entry control cards may be used instead of ECRs, providing the same information in (2) above, is contained in the control cards.

(4) Personnel issued a controlled picture badge need not be listed on an ECR when a badge exchange system is in use

7-3. Visitor controls

a. Control measures. Escorts or other internal control measures will be established to prevent unauthorized disclosure of, or access to, security interests in restricted areas.

b. Areas between fences. The responsible commander will establish visitor controls for the areas between the inner and outer perimeter fences of the site.

7-4. Package, material, and vehicle controls

a. A positive system will be used to control movement of packages, material, and vehicles into and out of limited areas. An electronic detection system should be used to enhance the controls. Searches and inspections for prohibited items and contraband will be conducted with FM 3-19.30 and this regulation. Inspection and search procedures will be coordinated with the supporting staff judge advocate for legal sufficiency.

b. The facility commander/director will establish search procedures for inspecting all personnel entering into or departing a chemical limited area to reduce the risk of unauthorized items being brought into or removed from the limited area. The following applies:

(1) For personnel requiring escort. Upon entering the limited area, all hand-carried items (that is, handbags, purses, brief or attaché cases and protective mask carriers) will be inspected by security personnel for readily detectable prohibited items and contraband. As applicable, hand-carried items leaving the limited area will be inspected for unauthorized removal of chemical agents.

(2) For personnel authorized unescorted access. The commander may authorize the use of random searches for personnel authorized unescorted access. As a minimum, at least one random search will be conducted monthly to validate the random search authorization.

c. Upon entering or leaving a limited area, all vehicles will be inspected by security personnel for unauthorized personnel and readily detectable prohibited and contraband items for items of particular concern). As a minimum, each vehicle will be given a visual inspection of readily accessible areas. For example—

- (1) The passenger compartment.
- (2) The cargo compartment.
- (3) The engine compartment.
- (4) The underside of the vehicle.

d. Sealed packages that cannot be inspected require a signed OF (7) (Individual Property Pass). The bearer of the sealed package will not sign the OF (7). It will be signed by another authorized individual. Persons authorized to sign OF (7) will be designated in writing by the responsible commander or designated representative. Samples of signatures of personnel authorized to sign OF (7) will be maintained at the exit control point. A locally generated form may be used for this purpose. Changes will be updated as necessary. Other packages and material not covered by OF (7) will be checked for unauthorized items. For packages, containers or vehicle compartments that cannot be safely inspected by security guards, a bill of lading, hazardous waste manifests, or DA Form 4508 (Ammunition Transfer Record) may be used in lieu of the OF 7. In either case the signatures must be verified.

e. Only essential military (or Government), emergency, and contractor vehicles and materials handling equipment will be permitted to enter limited areas.

f. Vehicles and material handling equipment remaining in limited or exclusion areas after duty hours will be secured to assure that they are not readily usable by a hostile force. This includes unattended vehicles or equipment left in the immediate vicinity of the site area. No vehicle or material handling equipment will be parked within the inner or outer clear zone.

g. Signs requiring removal of the ignition keys and locking of all vehicles will be placed at parking areas within 50 meters of facilities or areas containing chemical agents to include the interior of the chemical limited area. This requirement applies to Government, privately-owned, and commercial vehicles.

7-5. Opening of storage structures after duty hours

Except in an emergency, covered by local SOPs and before a chemical agent storage structure is opened after normal duty hours, authorization will be obtained from the commander/director or his/her designated representative who will verify the need for such entry. The term “duty officer” is defined in the Glossary. When such an opening is authorized, pertinent facts will be entered in the guard daily log. Each change of shift supervisor will review the daily log concerning entries addressing the opening of structures and, if deemed necessary because of the facts and circumstances, verify the validity of structure openings and such authorization for the opening of structures with appropriate command authorities (procedures will be established in guard orders or site physical security plans) to sample and verify that select instances of structure access/openings were properly authorized.

7-6. Security of open igloos

a. An open storage igloo containing chemical agents increases its vulnerability to a planned or opportunistic attack. The security system is momentarily weakened because the alarms, locks, and other protective devices, including the

door itself, are temporarily ineffective. To compensate for this security degradation, the approaches to open doors to igloos containing chemical agents will be kept under the surveillance of security patrols.

b. Use of security guards or observation devices monitored by security personnel, or other authorized people involved in the chemical operation having access to an integrated communication device, may be used to satisfy this requirement. Commanders will develop procedures to notify security guard personnel when chemical agent storage igloos are to be opened, so that roving security guard patrols can increase the random surveillance of the opened igloos.

7-7. Chemical Weapons Treaty Compliance Inspections

a. Applicability. These entry and exit control procedures will apply to inspectors, escorts, and other participating personnel during the conduct of official chemical weapons (CW) treaty on-site verification inspections of CW storage, CW production, and CW destruction facilities. The procedures will be incorporated in the Army Chemical Compliance Implementation Plan.

b. Identification and entry authorization. Upon arrival of the Treaty inspection personnel at the inspection site, the facility commander/director, or designated representative, will be provided with a validated roster listing each person on the Treaty inspection team, to include both Organization for the Prohibition of Chemical Weapons (OPCW) and U.S. personnel.

(1) The roster will be signed by the Defense Threat Reduction Agency (DTRA) Team Chief or Operations Officer or Sub-team Chief and countersigned by the facility commander/director or designated representative. The appropriate signature blocks will be typed or stamped on the roster.

(2) At this time, the DTRA Team Chief or Operations Officer or Sub-team Chief will be required to vouch to the facility commander/director or designated representative that members of the treaty inspection team have been identified, and that their hand-carried items have been inspected for prohibited items (for example, weapons and explosives). The approved equipment used by the inspection teams is authorized entry into the inspection site.

(3) The validated roster will serve as the entry control authorization document for entry to the inspection site.

(4) Badges issued by DTRA Team Chief or Operations Officer or Sub-team Chief to treaty inspection personnel, both OPCW and U.S., will be listed in the entry control rosters and used for entry to the inspection site.

(5) Badges for accompanying site personnel and escorts may be issued outside the inspection site, instead of at the site entry control facility, to expedite entry of the treaty inspection team. Strict badge accountability procedures will be enforced at all times. Personnel will be listed on properly validated site entry control rosters according to established procedures.

c. Entry procedures.

(1) The facility commander/director or designated representative will provide the site entry controller with the entry control rosters of the treaty inspection team and accompanying site personnel and escorts.

(2) The DTRA Team Chief or Operations Officer or Sub-team Chief will—

(a) Verify the identity of each person on the treaty inspection team listed on the entry control rosters.

(b) Verify that each person and their hand-carried items are free of prohibited items.

(3) The facility commander/director or designated representative will—

(a) Verify for each person accompanying or escorting the treaty inspection team listed on the entry control roster.

(b) Verify that each person and their hand-carried items are free of prohibited items.

(4) The entry controller will then allow entry of these personnel in the inspection site as a controlled group.

d. Exit procedures. Unauthorized removal of chemical agents from the inspection site is prohibited.

e. Vehicle control.

(1) Vehicles used to transport personnel into and out of the inspected site will be inspected by security personnel for unauthorized personnel and prohibited items prior to the vehicles being placed into such use.

(2) The vehicles will remain under security or escort control at all times to ensure the vehicles remain sanitized upon entering or exiting the inspection site. Vehicles which can not be under security control at all times will be inspected upon entering and exiting the inspection site.

(3) Security escorts accompanying the vehicles will verify with to the site entry controller that the vehicles have been inspected and sanitized.

(4) The entry controller will then allow the vehicles to enter or exit the inspection site without inspections.

f. Security escorts.

(1) Based upon the Commander's assessment, a sufficient number of security escorts will be provided to ensure a controlled security environment for the treaty inspection mission.

(2) The ratio of personnel to be escorted to the number of escort personnel will be such that escorting personnel can perform their surveillance and control duties satisfactorily.

g. Local procedures. Local, detailed security procedures will be developed and implemented by site commanders in support of the treaty inspection mission. The control procedures will preclude unauthorized access to security interests.

Chapter 8

Key and Lock Controls

8-1. Category I, II, or III chemical agents

The provisions of this chapter apply to category I, II, and III chemical agents' facilities. Surety keys and locks are those keys and locks that control access to chemical surety limited and exclusion areas.

8-2. Access and controls

a. Surety keys, locks, and lock combinations will be strictly controlled and accounted for at all times. These keys will be maintained separately from other keys and will be accessible only to those individuals whose official duties require access to them. Keys will not be left unattended or unsecured at any time.

b. The two-person concept described in the glossary of AR 50-6 applies to keys allowing access to chemical agents' exclusion areas. A key control system will be established so that no one will be allowed to interchange access to keys to installed "A" and "B" locks. This concept also applies when two locks are used to secure entry doors to rooms storing Category III chemical agents.

c. Although keys required for maintenance and repair of IDS, including keys to the control unit door and monitor cabinet, are not surety keys, they will be accessible only to authorized maintenance personnel. A list of authorized maintenance personnel will be kept current and accessible to personnel who control such keys. Key control registers will be required showing the disposition of the keys at all times. Procedures will be established which allow security personnel to know the disposition of the keys and to verify the alarm status of IDS locations accessed by maintenance personnel. Testing of IDS by security personnel is required immediately after maintenance, repairs, or modifications of IDS. Keyed alike systems are authorized for IDS control unit doors and monitor cabinets which themselves are protected by tamper devices.

d. A roster of personnel authorized to receive keys and combinations storage areas will be kept current by responsible organizations. The roster will be protected from public view. The roster will be signed by the Primary Key Custodian. Keys will not be duplicated unless authorized by the key control officer. Duplicated keys will be strictly accounted for at all times. Master keys and keyed-alike systems are prohibited except in the case of locks on manhole covers and culverts that penetrate the perimeter and perimeter fence gates. Such keyed alike systems will not be duplicated. Loss or compromise of such keys will result in immediate replacement of the affected locks, or change of lock cylinders and such actions will be recorded.

e. When not attended or in use, keys will be secured in a locked key container. Any GSA-approved security container, or equivalent container, or key container of at least 20-gauge steel, is acceptable for storing such keys. An appropriate locking system will be used to lock the key container. The key container will be located in a room where it is kept under surveillance or in a room that can be locked during non-duty hours.

f. An automated, lockable, key container is authorized provided the container meets GSA standards and generates a record of key usage. Ensure the electronic key container is properly programmed permitting only authorized personnel access to duty specific keys. A record of all daily transactions containing the name of the individual receiving the key, date and time of issuance and date and time returned will be printed at the end of each duty day or other time as appropriate. In case of a system failure, detailed instructions will be included in the lock and key standard operating procedure (SOP) on how accountability will be maintained and emergency access to the keys stored in the automated container. The key custodian will maintain records of transaction for 1 year.

g. When combinations or codes are used in lieu of keys, the control procedures used for keys will apply to maintain the integrity of the combinations or codes.

h. Keys and locks to installed locks will not be removed from the installation.

i. In the event of lost, misplaced, or stolen keys, the affected locks or cores to locks will be replaced immediately. Compromised lock combinations will be changed immediately.

j. Replacement of lock cylinders and broken keys to high-security locks will be requested by the key control officer through normal supply channels.

k. Locks will receive preventative maintenance as a minimum, semi-annually or more frequently as required. A record of maintenance will be maintained for 12 months.

l. Combinations to locks, when used, will be changed—

- (1) When placed in use.
- (2) When an individual knowing the combination no longer requires it.
- (3) When the combination has been subject to compromise.
- (4) At least every 12 months.

m. Lock combinations will be recorded, sealed in an envelope, and stored in a security container. No other written record of the combination will be kept. SF-700, Security Container Information, may be used to record the lock combinations. The integrity of the two-person rule will be maintained.

n. Padlocks will be locked to the hasp.

o. Reserve locks and keys will be secured at all times to preclude accessibility to unauthorized personnel.

p. Lock location rosters will be protected from unauthorized persons and will be maintained by the Primary/Alternate Key custodian.

q. Key control officers and locksmiths will not be authorized access to information concerning the specific locations of installed locks protecting chemical agents at the site (for example, specific storage igloos within a site). The intent of this requirement is to preclude the possible circumvention of the two-person control system by prior handling of these locks and keys.

r. Keys will be inventoried jointly with each change of custody and recorded. Keys in two-person controlled containers will be inventoried only when the containers have been opened.

s. Not more than every 90 days, a commissioned officer, Department of the Army civilian in the grade of GS-07 or above or a contractor employee in a supervisory position, appointed, in writing, by the commander concerned or designated representative, will inventory keys and locks by serial number. The person appointed to conduct the inventory will not have a vested interest in the outcome of the inventory. Inventories will be reported in writing to the key control officer. Inventories will show the general location of keys and locks, but not the exact location of each installed lock, for example, the specific storage structure involved. Inventory discrepancies will be resolved and reported to the commander concerned. The quarterly inventory requirement does not apply to keys to access/secure switches for IDS control unit doors located inside alarmed chemical agent storage structures. These keys functions as toggle switches to access/secure the IDS when the storage structure is opened and locked. Key inventory records will be kept in unit files for 12 months.

t. The person appointed to conduct the quarterly inventory will not have a vested interest in the outcome of the inventory. Inventories will be reported in writing to the key control officer. Inventories will include the general location of keys and locks, but not the exact location. Inventory discrepancies will be resolved with the key control officer (KCO) and any unresolved discrepancies will be reported to the commander concerned by the inventorying representative. The inventory will be accomplished by a commissioned officer, Department of the Army civilian, in grade of GS-7 or higher, or a designated contractor employee.

u. Key inventory records will be kept in unit files for 12 months.

v. The procedures for conducting the quarterly inventory are:

(1) Inventory officer will review the DA Form 2062, which lists all keys and locks introduced into the surety program.

(2) Inventory officer will review additional receipts for locks and keys that have been added to the system since initial receipt.

(3) Inventory officer will review any destruction documents for destroyed locks and keys. The inventory officer will then contact the custodians and physically see all remaining locks and keys that are in the system.

(4) The inventory officer will verify that all locks, keys and serial numbers on the initial DA Form 2062, Hand Receipt/Annex Number, have been accounted for or destroyed.

(5) Key control registers will contain the information listed in (a) through (e) below. DA Form 5513-R, (Key Control Register and Inventory), may be used to meet this requirement. DA Form 5513-R may be reproduced locally on 8½ X 11-inch paper. Completed key registers will be retained in the unit files for at least 90 days. Include the following in the key control register:

(a) Serial number. Locks or keys which do not have a serial number will be given one. This number will be inscribed on the lock or key as appropriate.

(b) Printed name and signature of the individual receiving the key.

(c) Printed name and signature of the person issuing the key.

(d) Date and time of issuance, and date and time returned.

(e) Printed name and signature of the individual receiving the returned key.

8-3. Lock rotation

a. Key padlocks will be changed, have their cylinders replaced, or be rotated randomly between storage structures or sites at least every 12 months. This requirement also applies to key padlocks on perimeter gates which do not have authorized keyed alike locks and key padlocks on manhole covers which permit entry to the protected area. Such changes will be recorded and retained in unit files for 12 months.

b. The rotation of padlocks will not be required when two locks are installed on each chemical agent structure and a system is set up for separating these locks into "A" and "B" locks. Personnel will be identified and authorized access only to either "A" or "B" lock keys (or combinations), but not both. The system will preclude an individual from interchanging access to the "A" and "B" keys.

8-4. Key control officer

a. The KCO will be in the PRP program and will be appointed in writing by the commander/director to manage the key and lock control system. The commander/director may appoint an alternate key control officer.

b. The key control officer's duties will include—

(1) Procurement and initial receipt of keys and locks through supply channels.

(2) Maintenance of records to identify each key and lock used by the activity, including replacement of reserve keys and locks. Accountability from receipt to disposal (chain of custody) of such keys and locks will be required. The current area location and custody of each key and lock will be shown in such records. Records showing the exact locations where such keys and locks have been placed in use will not be maintained by the key control officer. Such records will be maintained by the key custodians who actually possess the keys (for example, security force, operations, and so forth).

(3) Issuance of keys and locks to key custodians at the storage site or activity will be by utilizing DA Form 2062, Hand Receipt/ Annex Number or a locally developed automated form providing that this form contains all the required information from the DA Form 2062.

(4) Keys and locks subject to the two person rule will not be placed in use at the facility by the key control officer. Such keys and locks will be placed in use by the respective key custodians. Additionally, the key control officer and locksmiths are not authorized access to such keys while the locks are in use under the two-person rule.

(5) Backup spare locks and keys for the lock system will be stored and accounted for at all times. These spare locks and keys will be issued to the custodians when the custodians have the appropriate means to secure them.

(6) Investigation of lost, stolen, or unaccounted for keys.

(7) Maintenance of an updated list of designated key and lock custodians for the storage site or chemical activity.

(8) Establishment and maintenance of an up-to-date key and lock control SOP to ensure the effective management of the key and lock control procedures prescribed in this chapter.

c. The alternate KCO will be able to perform the same duties as the primary KCO in the absence of the primary KCO. The lock and key SOP will list detailed procedures for transferring duties and lock and keys between the primary and alternate KCO in both regular and emergency situations.

d. Procedures for transferring duties and control of keys and locks between the KCO and the alternate KCO will be clearly delineated in the key and lock control SOP. At a minimum, a 100 percent inventory will be conducted of all paperwork for issued keys and locks, a 100 percent physical inventory of reserve keys and locks on hand. The alternate KCO will assume control after signing the DA Form 2062.

8-5. Key custodian

a. Key custodians will be in the PRP program and will be appointed in writing by the commander/director concerned or designated representative to manage the key and lock control system within their designated area. The commander or designated representative may also appoint an alternate key custodian.

b. The key custodian's duties will include—

(1) Procuring locks and keys from the KCO.

(2) Maintenance of records to identify each key and lock used in their designated area, including reserve locks and keys. Accountability of all keys and locks will be required. Maintain a roster showing the exact location of all keys and locks. This roster will not be provided to the KCO or locksmith.

(3) Issuance and receipt of any keys.

(4) Ensuring that the list of authorized personnel to sign for keys is kept up to date, signed by the commander/director or designated representative, and stored near the respective key box.

(5) Securing reserve locks and keys in accordance with this regulation. If unable to store appropriately, then coordination will be made with the KCO to secure reserve locks and keys.

(6) Reporting any lost stolen or unaccounted locks or keys to the KCO immediately.

Chapter 9 Security Forces

9-1. Category I or II chemical agents

The provisions of this chapter are applicable to category I or II chemical agent storage sites.

9-2. Qualifications of security force personnel

a. Commanders will ensure that only personnel who are best qualified, physically fit, trained, capable, reliable, and trustworthy are used to protect chemical agents. Standards in AR 190-56 are applicable to civilian security guards assigned to chemical agent security duties.

b. Commanders will take necessary actions to ensure that guards who do not meet chemical PRP requirements are

not assigned to chemical storage sites. Security guard force personnel who are working outside the chemical limited area may still be part of the chemical limited area Response Force but do not require PRP Certification.

c. Security guards not in the PRP must still meet the requirements of the individual reliability program (IRP) annotated in AR 190–56.

9–3. Guard motivation requirements

a. *Forbidden materials on post.* In general, guard post will be forbidden the use of recreational materials, such as radios, books, magazines, games, and television sets. However, security force and custodial personnel performing duties which do not involve detection and assessment functions may be permitted their use providing they do not interfere with their duties.

b. *Working environment.* Measures, where possible, which can be taken to alleviate the tedium of the security function include the following:

- (1) Standardized and advanced schedules for work and leave.
- (2) Frequent rotation of static posts during each shift.
- (3) Hot meals during all tours of duty.

c. *Nonsecurity functions.* Security force personnel will not be tasked to perform other than security functions while on duty.

d. *Overtime.* Commanders will monitor and evaluate overtime hours and take appropriate action to preclude excessive overtime by guards.

9–4. Guard orders

Written guard orders will be provided for each post and patrol. Guard orders will either be carried by the guard or be available on the site for use by guards. The orders for each post and patrol will be worded clearly and concisely, and be easily understood. The orders will include instructions for the use of force according to AR 190–14. Commanders will ensure that guards thoroughly understand the orders for their posts and patrols before assuming such duties.

9–5. Security forces and use of Force

a. A security force will be established to perform the physical security requirements outlined in this regulation, in the security plan, and in applicable regulations. Security guards sufficient to control entry and to prevent unauthorized access to chemical agents, along with backup forces capable of responding to attempted penetrations and preventing unauthorized removal of chemical agents, will be in place at all sites 24 hours a day. The actual number of security force personnel will be specified in the site security plan.

b. Chemical facility commanders/directors will ensure sufficient security forces are available to fulfill necessary security requirements outlined in this regulation.

c. Chemical Agents are designated as inherently dangerous to others. The use of deadly force is authorized in accordance with AR 190–14.

d. Commanders will ensure that all assigned civilian security forces meet the requirements in AR 190–56 and are flexible enough to adjust to Force Protection Conditions requirements established in AR 525–13.

e. Police.

Security Forces that meet the following must be in the PRP:

- (1) Have direct access to chemical agents.
- (2) Control direct access to chemical agents.
- (3) Issue proximity cards, PIN, keys, combinations, biometric codes, or any other mechanisms that provide direct access to chemical agents.

9–6. Response force

a. The RF will be comprised of a sufficient number of armed security personnel capable of preventing, containing, neutralizing, and repelling intrusions or unauthorized activity within the established time limits.

b. The size and composition of the RF at a particular site will be determined by an analysis and evaluation of the operational mission, facility configuration (to include size of site, terrain, and so forth), postulated threat, local security threat, vulnerability assessment, and results of force-on-force training.

c. The actual size and composition of the RF will be recommended by major subordinate commander and approved by the SMC. All changes to existing RF manpower requirements will require documented justification and approval by the SMC before such changes are made.

d. The following requirements apply:

- (1) Requests will include a detailed analysis.
- (2) Provide a copy of the site security plan and documented vulnerability assessment conducted according to requirements specified in chapter 16.
- (3) The commander's endorsement will include comments that the proposed size and composition of the RF was

assessed for adequacy from a command perspective, taking into consideration the RF mission requirements in this regulation and the security risks and associated threats involving chemical agents.

(4) Commanders at all levels of command will take appropriate action when requests are not in consonance with these requirements.

(5) At the SMC level, the requirement for commanders to endorse the requests may be delegated to a general officer (or equivalent Senior Executive Service civilian) assigned to that headquarters.

e. The RF will be organized and trained to operate as tactical elements to permit their optimal use and flexibility. Elements of the RF may—

(1) Patrol the storage area.

(2) Assess alarms that cannot otherwise be evaluated.

(3) Act as the immediate response force capable of responding to a threat situation within prescribed time limits.

f. The RF may be employed as a single unit or in several elements. In either case total reaction time of the RF will not exceed 30 minutes after notification of the alarm or threat situation.

(1) Designated members of the RF will respond within 15 minutes to assess the alarm or threat situation.

(2) They will be reinforced by designated members of the RF who will respond to the alarm or threat situation within the time determined by the commander, but will not exceed the total RF reaction time of 30 minutes.

(3) Provisions will be made to counter multiple intrusions on installations having more than one chemical agent storage facility to be protected.

g. A portion of the RF will be deployed in a random manner in either fixed observation or fighting positions, and as mobile foot or vehicle patrols. Random deployment is an active security measure which enhances the security posture by reducing the attacking force's ability to pin down or delay RF deployment. Increasing RF detection capability adds an unknown element that the attacker must contend with prior to the start of the attack and helps to negate the element of surprise on the part of the attacker. The number of RF personnel engaged in random patrol or fixed fighting positions will be determined by the security force commander. Random patrols or fixed positions may be established both inside and outside the limited area. Random employment of the RF ensures that a set deployment pattern is not established.

h. The tactical employment of the RF will rely on basic combat skills. The tactical application of the RF will be directed to the day-to-day security requirements.

i. At least once each month the RF will undergo training exercises to maintain proficiency. The RF will be evaluated continuously to ensure it meets the prescribed time limits. Evaluation, however, should never be by the "stop watch" approach. The evaluation will consider whether the RF deployed in a tactically sound manner or denied access to the intruder(s) by laying a base of fire. The evaluation will also consider whether the RF avoided delay or defeat by diversionary tactics or ambush.

j. The RF will be organized and trained to operate either as tactical elements or as a total RF. The posted sentries (for example, entry and access control, tower guards) will not be a part of the RF numerical requirement, and will continue their assigned tasks when the RF is deployed. The purpose of this organization and training is to permit maximum utilization and flexibility of members assigned to the RF. Elements of the RF may be deployed to patrol the storage or alert area, assess alarms which cannot be otherwise assessed, act as the initial contingent of the RF until the total force arrives should it be needed, or perform other security functions providing they do not degrade the primary functional capability of the total RF. In no case will the capability for response of the total RF exceed 30 minutes from the time a determination has been made to commit the force.

9-7. Augmentation force

a. The augmentation force (AF) will be organized and structured to provide a force that is responsive to the needs of the installation or activity being supported. The SMC will determine the actual number of personnel required, and will identify the organization that will provide the AF. The AF, its location, and the method of contacting the AF will be included in the physical security plan or site defense plan.

b. Reaction time for the AF will be set by the SMC. Response will be based on actual or anticipated threat, and the geographical location of the supporting force.

c. When requested by SMC with custody of chemical surety materials, CG, FORSCOM, will prescribe the AF size and response time requirements. CG, U.S. Army Training and Doctrine Command (TRADOC) will provide support when requested by CG, FORSCOM.

d. The AF will train as often as necessary to maintain proficiency.

e. The AF will be exercised every 12 months at the supported storage facility. The SMC may deviate from the requirement to conduct such exercises at the supported storage facility when it is not economically feasible. In such cases, selected key staff personnel of organizations providing the AF support will be required to physically visit the storage facilities to which they provide such support, and prepare and train their subordinate units to meet requirements. The cost of such exercises and staff visits will be borne by the supported unit.

9-8. Records of test exercises

Records of test exercises will be maintained for 12 months. A narrative assessment of response capabilities will be included, as well as the number of security force personnel involved in the exercises.

9-9. Security force weapons and equipment

a. Weapons.

(1) Provide security forces availability to weapons with the maximum practical firepower provided for security forces operations. Sidearms have little value as protection from dedicated adversaries except in confined quarters. Where it is determined to be necessary or advisable to issue sidearms to personnel responsible for protection of chemical agents, weapons providing greater firepower will also be immediately available to them.

(2) The security force will be equipped and armed for combat type operations and terrorist incidents. The site vulnerability assessment and local surrounding environment will be considered in authorizing the types of weapons to be employed. The below listed weapons or comparable types, will be considered for use—

- (a) M16 rifle.
- (b) M4 carbine.
- (c) M60 machine gun.
- (d) M2 .50 caliber machine gun.
- (e) M203 or M79 40 mm grenade launcher.
- (f) M249 squad automatic weapon.
- (g) M9 9 mm pistol.
- (h) Shotgun.

b. Equipment.

(1) Security and response forces and convoy escort personnel will have provided the maximum protection feasible. At a minimum, protective mask, protective body armor, and helmets will be immediately available to response forces. Protective masks will be available to all.

(2) In areas of difficult terrain or subject to adverse weather, a capability for cross-country travel over this terrain or snow will be available to the RFs.

(3) Commander will conduct as a continuing objective, analysis of the condition and readiness of the security guard fleet's motor vehicle reliability and take appropriate action to ensure vehicle readiness. This requirement will be subject to oversight review during physical security inspections.

(4) When response is normally on foot, vehicles (surface and/or air) will be designated for use by RFs in the event of operational necessity.

(5) A vehicle which will provide protection against small arms fire will be provided at locations deemed appropriate by the commander concerned based on the site vulnerability assessment, to include the security threat, size and topography of the area, and location of all members of the security force.

(6) RFs normally stationed outside storage areas will have wire cutters or bolt cutters issued as a part of their equipment in order to cut through fences should the normal entry gates not be available for use.

(7) Non-lethal riot control agents and other less lethal force options should be available for use by the security forces. Security personnel will be trained on non-lethal systems prior to use.

c. Security of weapons and ammunition. To ensure security force weapons and ammunition have not been tampered with and made unserviceable when needed, the following precautions will be taken—

(1) Security force weapons will be randomly checked for serviceability, including such weapon parts as firing pins, extractors, and so forth.

(2) Magazines or ammunition clips will be randomly unloaded and the rounds inspected. Ammunition, both loose and bulk, will be randomly checked for tampering.

(3) The random checks of weapons and ammunition will be performed by personnel other than those personnel (for example, arms room personnel) who routinely issue such weapons and ammunition to security forces.

9-10. Tactical defense deployment

a. Protection of chemical agents will be based upon sound tactical defense planning. The commander and security officer will identify vulnerabilities and probable targets on the storage facility, and include these in the site tactical defense plan. Tactical planning will take into consideration such things as cover and concealment of both friendly and hostile forces, natural terrain that can be used for deploying forces, and barrier and fighting positions. Enough barriers and fighting positions will be built to increase protection and ease of deployment for the security force.

b. The RF and AF will deploy in a tactical manner involving fire and maneuver. Preplanned weapons fire will be set up for the final defense of the storage facility. Protection of avenues of approach for reacting forces will be included in planning.

c. Care will be taken to ensure that responding forces do not use avenues of approach through an area which would make them vulnerable to attacking forces.

9–11. Site area searches

Security patrols will conduct searches in all areas of possible concealment around the site (depending on jurisdictional authority) for indications of use of such areas for observation and surveillance of site operations by unauthorized personnel. While searches on foot would be most productive, other methods may be applied as determined by the local commander and site peculiarities. Searches will be thorough, conducted at random times by random routes, and accomplished at least once weekly.

9–12. Operations security

Every effort will be made to conduct as many site operations as possible in a random manner. The purpose of random operations is to reduce or eliminate any audio or visual patterns that may be detectable from outside the site. Principles and objectives of OPSEC in AR 530–1 apply.

a. Examples of operations that should be randomized include—

- (1) Manning of towers and fighting positions.
- (2) Numbers and routes of patrols.
- (3) Shift changes.
- (4) Storage structure door openings.
- (5) Chemical agent movements.

b. Increase the random operations when information is received that a particular installation may be targeted for an incident or attack.

c. Enforce strict communications discipline for all radio and landline transmissions on the security force communications net. Local operating instructions will require all posted security forces to report to a central communications control or its equivalent. Security forces will report as often as needed to verify the communication net's operability and functional integrity. When operationally feasible, communications checks will include a degree of randomness.

9–13. Site and perimeter patrols

Assigned security forces will periodically check the perimeter to assure site integrity (for example, no breaks in fence line, no evidence of attempted penetrations). Surveillance by patrols will include checking vulnerable features of the limited area, storage structures, and exterior openings (gates, culverts, doors, and windows), despite protective metal grills or bars on these openings. The frequency and type of patrol checks depends on the threat, vulnerability, and physical layout of the site. Each patrol vehicle will be equipped with an appropriate auxiliary light for use during the hours of darkness. Flashlights and night vision devices will be readily available for use by security patrols during the hours of darkness.

9–14. Control of demonstrations

a. Security forces designated to protect chemical agent storage sites will not become directly involved in controlling demonstrations outside the outer perimeter barrier. However, deadly force measures may be employed where appropriate. Commanders will coordinate and execute a written and signed memorandum of understanding with local civil or military authorities (local police or provost marshal) for such support. Local intelligence units will provide notification of pending demonstrations as soon as information on these demonstrations becomes available.

b. Commanders will ensure that security force personnel are knowledgeable and trained in controlling demonstrators once the outer fence is penetrated. Commanders will ensure this training is evaluated at least every 12 months.

c. Because of the extremely sensitive and unpredictable nature of demonstration, security force training on the use of deadly force needs to be reinforced during the incident. When confrontations with demonstrators appear likely, security forces will be given specific instructions on the use of deadly force based on the circumstances of the particular situation. The mere act of breaching (trespassing) the limited area by demonstrators who allege a peaceful purpose will not in and of itself be a basis for the use of deadly force. However, if a determination is made that the ultimate purpose of the demonstration or selected demonstrators is to damage, steal, or seize chemical agents and all lesser means have failed, selected employment of deadly force measures may be employed to stop these acts. If time permits before a demonstration, the responsible commander will ensure that a designated chain of command is on hand, and that the entire security force understands which individuals are authorized to direct the employment of deadly force. The provisions of Executive Order 12333 and AR 381–10 apply to restrictions on the collection of information about U.S. persons.

9–15. Tactical deployment in response to alarms

a. *Flexibility.* Responsible local commanders must develop tactics, taking into consideration unique physical conditions, both natural and man-made. Commanders must exercise initiative and use innovation to tailor tactics in such a

manner as to retain that flexibility required in a defensive situation in which the potential enemy is postulated to have a wide range of attack options.

b. Capability. Realizing that the limited area is a potential battleground, the RF must have the capability to respond rapidly, in accordance with sound tactical concepts, regardless of the organizational structure (elements) of the RF.

c. Adjustment of security plans. Commanders concerned will continually review and adjust their local security plans and be prepared to respond in a tactically sound manner to a number of scenarios according to the site vulnerability assessment.

d. Threat scenarios. Commanders concerned will develop plausible, likely threat scenarios, and interface these scenarios with local security plans. The security plans and response tactics will be adjusted as required.

e. Tactical skills. The tactical employment of the security force will rely on the basic combat skills of soldiers. The tactical application of the security mission will be directed to both the day-to-day security requirements and the wartime mission. Security forces will be equipped and trained in ground and air defense.

f. Emergency situations. In emergency situations, the primary effort of all security forces will be directed to protecting the areas in which chemical agents are stored.

9–16. Unannounced aircraft landings

The RF will immediately respond when a helicopter or other aircraft lands unannounced on a chemical agent storage site area. When the helicopter or other aircraft lands adjacent to the chemical agent storage area, the RF will be alerted and respond to protect the site.

9–17. Guard logs

Guard logs will be maintained to record the chronology of events during the guard shift.

Chapter 10 Training

10–1. Category I and II chemical storage sites

a. The provisions of this chapter apply to security personnel assigned to category I or II chemical agent storage sites.

b. Training requirements for category III chemical agent security personnel will be tailored to meet mission requirements.

10–2. Training requirements

Personnel assigned to chemical agent security duties will receive basic and continuing training to ensure they are adequately trained and qualified to perform assigned duties. Training will be comprehensive and consist of both formal classroom training and practical exercises. Minimum training standards in AR 190–56 are applicable to civilian guards assigned to chemical agent security duties.

10–3. Basic training program.

Commanders will establish a basic training program to meet the requirements of this chapter. The program will include the following training subjects:

a. General training.

(1) Personnel identification.

(2) Circulation control: how personnel within the storage site or area are identified and controlled, to include escort requirements and procedures for duress situation.

(3) Apprehension.

(4) Operation, use, and testing of IDS equipment.

(5) Search and seizure (individuals, packages, and vehicles).

(6) Operation and use of primary and alternate security communications systems and equipment.

(7) Operation and procedures for starting emergency generators when automatic system fails. In the event that the emergency generator is computer controlled and must have properly certified/trained maintenance personnel to restart the generator, instructions must be in place that address the procedures for notifying properly trained maintenance personnel during non duty hours and after duty hours/weekends and holidays.

(8) Adversary threat (for example, terrorism, sabotage, espionage, theft, loss or diversion, civil disturbances, demonstrations).

(a) Adversary groups (to include insiders).

(b) Motivation and objectives.

(c) Tactics.

- (d) Recognition of sabotage related devices and equipment.
- (9) Security vehicle operations.
- (10) Duress system.
- (11) Security awareness and vigilance.
- (12) Record-keeping.
- (13) Type and location of hazardous and vulnerable equipment and materiel.
- (14) Location and use of fire protection equipment, utility switches, and first aid facilities.
- (15) Protective measures against chemical attack, self-aid, and first-aid measures.
- (16) Identification of chemical agents (recognition of such items in case of attempted unauthorized removal from the site or area).

b. Security skills training.

- (1) Small unit combat tactics (day and night).
- (2) Antiterrorism tactics.
- (3) Specialized equipment (for example, protective masks, body armor, night vision devices, radio communications, metal detectors, and so forth).
- (4) Use of force (including deadly force).
- (5) Site defense plans.
- (6) Weapons qualification with assigned weapons to include familiarization fire for weapons without formal courses of fire.

c. Transportation security (when applicable).

- (1) Convoy techniques.
- (2) Escort vehicle procedures.
- (3) General tactics for responding to threats.
- (4) Continuous surveillance of shipment procedures.
- (5) Isolation of shipment (load) vehicle.

d. Security supervisory personnel training.

- (1) Site defense plan.
- (a) Bomb threats.
- (b) Civil disturbances/demonstrations.
- (c) Hostage situations.
- (d) Motivation of security personnel.
- (e) Evaluation and uses of intelligence services.
- (2) Chemical agent recapture and recovery operations.
- (a) Recapture and recovery plan.
- (b) Interaction with other military or civilian recovery forces.
- (3) Emergency reporting requirements.

10-4. Specialized training

a. Security force personnel also will receive specialized training pertaining to their specific duties and duty location. This training will be certified in the training record by a supervisory level individual designated by the commander for this purpose, indicating that the individual is proficient for duty.

b. As a minimum, the following personnel will receive and be certified in the Specialized Training Program:

- (1) Security Desk Sergeant Operations.
- (2) Intrusion Detection System (IDS) Operators and Maintenance personnel.
- (3) Key Control Officers and Custodians, if part of the security force.
- (4) Special Reaction Team (SRT) members.
- (5) Personnel controlling entry into the chemical limited area.
- (6) Armorers, if assigned.
- (7) Shift Supervisors

10-5. Continuing training

Commanders also will establish a continuing training program to ensure all security personnel are able to perform routine duties competently and to meet emergencies quickly and efficiently. The program will include—

- a.* Refresher training in basic subjects.
- b.* Frequent firing of assigned weapons.
- c.* Briefings on security incidents of interest which have occurred at chemical agent sites.
- d.* Current and potential threats.

- e.* Intelligence and counterintelligence information.
- f.* Postulated actions by possible intruders and the planned security force reactions.
- g.* Practical exercises in defensive techniques to counter the threat.

10-6. Training records

Training records will be maintained on each individual assigned to site security duties. These records will be of sufficient depth, as determined by the commander, to ensure that the individual is qualified for certification and has maintained that qualification.

10-7. Force-on-force training

- a.* Force-on-force training exercises will be conducted to improve and maintain the proficiency of responding site security forces. These exercises are probably the most realistic method of evaluating the tactical defense plan.
- b.* Force-on-force training will be provided at least every 18 months for security forces at all locations where bulk chemical agents are stored or deployed. The training will be tailored to each location based on the DA postulated security threat and vulnerability assessment.
- c.* The training will include realistic force-on-force exercises using an engagement simulation system, and employing a trained aggressor force, when available, or local forces which will act as the aggressor for the exercises.
- d.* The training may be conducted on-site or at off-site locations when required by critical security and safety considerations. Continuous security of the site will be maintained at all times during such exercises.
- e.* Feedback from force-on-force exercises will be provided to all site security personnel.
- f.* All force-on-force training will be documented and made available for review and inspection.

10-8. Weapons training

- a.* Security personnel will receive training so they will thoroughly know the weapons with which they are armed, to include the proper care, maintenance, safety features, malfunctioning, and corrective actions.
- b.* SMC will prescribe the frequency of training in live fire of weapons to ensure acceptable levels of weapon proficiency are developed for security forces armed with such weapons. Requirements in DA Pam 350-38 and AR 190-56 will be used as guidance. Night firing should be conducted as part of live fire weapons training when there is reasonable access to adequate range facilities for this purpose.
- c.* The security force will be cross-trained and familiar with all weapons available to the security force.

10-9. Training evaluation

Commanders will determine the adequacy of the security training program through periodic evaluation of security force proficiency during response exercises and while on duty at fixed posts and mobile patrols. Adjustments to the training program will be made accordingly.

Chapter 11 Transportation Security

11-1. All categories of chemical agents

- a.* The provisions of this chapter apply to all categories of chemical agents.
- b.* AR 50-6 is the controlling directive for policies and procedures for the transportation and movement of all chemical agents.
- c.* The security provisions of this chapter are intended to complement the policies and procedures set forth in AR 50-6.
- d.* Temporary exclusion areas will be established when chemical agents are removed from storage structures for transportation or movement (chemical agents that do not exceed the chemical surety threshold quantity levels in AR 50-6 are excluded from this requirement).

11-2. Off-post movement of chemical agents in quantities greater than category III

- a.* The movement plans required in AR 50-6 for off-post movement of chemical agents in quantities greater than category III will contain provisions for sufficient security forces to ensure protection of the chemical agents during the movement.
- b.* The size and composition of the security force will be determined by the method of transportation mode used to transport the chemical agents (for example, aircraft, ship, rail, or motor vehicle), taking into consideration the area to be traversed and other pertinent security considerations. For example, in the case of ground movement by motor vehicle, the travel distance and time involved, road configuration, nature of the surrounding terrain (heavily wooded, high ground), day or night movement, as well as the postulated threat and local security threat will be considered in

developing the required movement plans specified in AR 50–6. The actual size and composition of the security force will be included in the movement plan which will be submitted for approval according to procedures in AR 50–6. The plan may be for a particular movement or continuing movements, as required.

11–3. Off-post and on-post movements of category III chemical agents

Escorting requirements for movement of category III RDTE chemical agents are contained in chapter 7, AR 50–6.

11–4. On-post movements of category III or greater chemical agents between limited areas involving chemical demilitarization operations

a. When demilitarization facilities are not co-located within the limited area of chemical storage depots, a standing operating procedures (SOP) movement plan will be required to ensure adequate security is provided for chemical agent movements between the respective limited areas. The plan will be developed by the local commander and approved by the next higher commander or SES equivalent at the MSC. An individual plan is not required for each movement. The intent is to implement a plan which will cover the daily and continuing chemical agent movements between the respective limited areas in support of the demilitarization mission.

b. The security considerations outlined in paragraph 11–2, above, will be used to determine the number of guards that will accompany the chemical agent movements while in-transit between limited areas. The plan will also include provisions for backup security forces to support the mission.

11–5. Movements of recovered chemical warfare materials

a. Movements of actual or suspected chemical warfare materials that are recovered from locations outside of chemical agent authorized storage sites will be accomplished according to AR 50–6.

b. Depending on the nature and sensitivity of the recovery mission and chemical warfare materials involved, the on-scene commander of the recovery operation will make the decision whether or not to arm the required escort personnel accompanying the chemical warfare materials to the designated storage destination(s).

11–6. Requests for additional security guidance

Commanders may request security guidance for transportation or movement of chemical agents in cases not specifically covered in AR 50–6 or this regulation. The requests will be forwarded through command channels to ATTN: Office of the Provost Marshal General (DAPM–MPD–PS), 2800 Army Pentagon, Washington, DC 20310–2800.

Chapter 12

Chemical Agent Recapture and Recovery Operations Planning

12–1. All categories of chemical agents

a. The provisions of this chapter apply to all categories of chemical agents.

b. Recapture refers to regaining custody of chemical agents which are in the possession of unauthorized persons. In this situation the chemical agents are assumed to be within a limited or exclusion area either in a storage structure or in the open.

c. Recovery refers to locating, if necessary, and to regaining the custody and control of chemical agents which have been captured and removed from custodial control.

12–2. Procedures

a. In the event of capture or removal of chemical agents by unauthorized persons, plans will be maintained at each chemical storage facility for the recapture or recovery of the chemical agents.

b. All necessary actions, including the use of deadly force, will be taken to recapture or recover chemical agents. Actions to recapture or recover chemical agents will be taken promptly or immediately upon availability of needed resources.

c. The presence of hostages will not deter the taking of decisive action to prevent unauthorized access to or capture or removal of chemical agents. The welfare and safety of any hostages will be considered in determining specific actions to take, but in all instances, the security of chemical agents will be paramount.

12–3. Planning

a. SMC with chemical agent custodial or storage responsibilities will develop and publish overall plans and guidance for the recapture and recovery of seized or stolen chemical agents. Plans will include forces to be used and rules of engagement. Incident reporting procedures will also be included. SMC will ensure such plans and guidance are integrated with each facility plan.

b. Recapture and recovery plans will be prepared for each chemical storage facility. Plans will include specific actions to take, procedures to follow, personnel required, tactics, and weapons to use for all likely situations or

scenarios for the site and chemical agents concerned. Coordination with local law enforcement agencies will be included in such plans.

c. Each chemical storage facility location will conduct annual recapture training for security forces. Recovery operations plans will be exercised according to SMC guidance.

12-4. Secure voice radio

Secure voice radio requirements in paragraph 6-4d apply for missions involving chemical agent recovery operations. This requirement does not apply to contractor-owned, contractor-operated activities.

Chapter 13

Category III RDTE Chemical Agents at On Post Locations

13-1. Category III RDTE chemical agent general requirements

The provisions of this chapter will apply to category III RDTE chemical agents that are used, stored, or produced for RDTE projects or other authorized purposes at on post locations.

13-2. Limited/exclusion areas

Chemical agents will be secured in an exclusion area within a limited area. The areas will be designated in the facility security plan according to the following criteria—

- a. The limited area will be designated as the inside of a room or laboratory containing a chemical secure container.
- b. The exclusion area will be designated as the inside of a chemical secure container.
- c. A temporary exclusion area will be designated when chemical agents are removed from the chemical secure container. The temporary exclusion area for this purpose will be the area immediately surrounding the chemical agents. In the absence of positive measures to prevent physical access by unauthorized persons, access to the temporary exclusion area will constitute access to the chemical agents.

13-3. Vulnerability assessment

a. A vulnerability assessment will be conducted at facilities where chemical agents are stored or used, in accordance with requirements in chapter 16 of this regulation. The vulnerability assessment may be modified to conform to the physical layout and surrounding environment of the facility.

b. The DA Implementing Instructions to the DOD Postulated Threat to chemical agents, and DA and SMC annual threat statements will be used in conjunction with the facility vulnerability assessment.

13-4. Storage containers

a. Chemical agents will be stored in any of the following chemical secure containers:

- (1) Laboratory hoods, freezers, or refrigerators.
- (2) Locally fabricated containers of at least 20 gauge steel, or material of equivalent strength.
- (3) Built-in containers constructed of at least 20 gauge steel, or material of equivalent strength, mounted in concrete at counter top level.
- (4) Security containers, vaults, safes, or vault-type rooms described in AR 380-5, for storage of classified material (any classification designation).

b. The following requirements will apply to chemical agents stored in laboratory hoods—

(1) Laboratory hoods with glass will be protected with steel mesh panels with a grid of not more than 1-inch by 2-inches center to center that can be raised or moved for authorized access to the chemical agents inside the laboratory hoods. The standard specifications for Steel Expanded Metal (F 1267) adopted by the American Society for Testing and Materials, 191 Race Street, Philadelphia, PA 19103, may be used to meet the steel mesh panel requirement. Installation of steel mesh panels on laboratory hoods will meet local safety requirements.

(2) Steel mesh panels are not required to be installed on the face of laboratory hoods when built-in containers described in paragraph 13-4 a(3), above, are used to store chemical agents inside laboratory hoods.

(3) All chemical secure containers, regardless of type, will be secured with two locks. Military specifications for medium security padlocks have been cancelled (see http://locks.nfesc.navy.mil/gfsp_introduction.htm). Medium security padlocks are authorized for continued use to secure all categories III RDTE chemical agents only until stocks are depleted or replacement is necessary.

c. At a minimum, containers will be secured with two General Services Administration (GSA) approved changeable three-position padlocks built to Federal Specification FF-P-110, or GSA-approved built-in combination lock, or a mix of two of these types of locks.

d. Hasp and staples for padlocks will be of heavy pattern steel, securely fastened to the structure with smooth head bolts, heavy duty rivets, or welding.

e. New construction or modifications of existing chemical agent laboratories will include installation of built-in vaults for chemical agents stored inside laboratory storage hoods.

f. Chemical secure containers will be stored in rooms meeting the construction standards outlined in paragraph 13–5, below, of this regulation.

13–5. Rooms or laboratories

a. Walls, floors, and ceilings will be constructed of at least ½-inch plywood, 1-inch tongue-in-groove wall boards or the equivalent. Roofs with suspended ceilings will be protected to ensure the crawl space cannot be used for covert entry.

b. Windows and openings (for example, conduits, vents, and ducts) in excess of 96 square inches with a smallest dimension greater than 6 inches will be barred or grilled to ensure a degree of security comparable to that provided by the walls of the room or laboratory.

c. Doors will be constructed of solid core wood or metal, possess the appropriate Underwriters Laboratory (UL) fire rating, and be designed to complement the security provided by the exterior walls of such rooms/laboratories. Hinges should be mounted inside the room/laboratory, or, if this is not possible, hinges mounted outside such rooms/laboratories will be welded, peened, or brazed to preclude removal from outside the door. Doors not used for primary entrance will be secured from the inside at all times and devoid of external locking hardware. Such doors will be equipped with appropriate hardware to permit rapid exit from the room/laboratory in the event of fire or other emergency.

d. Military specifications for medium security padlocks have been cancelled (see http://locks.nfesc.navy.mil/gfsp_introduction.htm). Medium security padlocks are authorized for continued use to secure all categories III RDTE chemical agents only until local stocks are depleted or replacement is necessary. The main entrance door to the chemical agent room or laboratory will be secured with a minimum of two key-operated deadbolt locks (with a 1-inch throw), or two General Services Administration (GSA) approved changeable three-position padlocks built to Federal Specification FF–P–110, or a GSA-approved built-in combination lock, or a mix of two of these types of locks. Padlocks will be mounted on comparable hasps.

e. All other doors will be locked from the inside with a deadbolt locking device (minimum of 1-inch throw), crossbar, or similar barrier resistant to manipulation from the outside. Panic hardware, when required, will be installed so as to prevent opening the door by fish-wire operation of the bolt from outside the door.

13–6. Exterior doors of buildings

Exterior doors of buildings which house rooms or laboratories containing chemical agents will be provided with an appropriate locking device on each door.

13–7. Security construction verification

Security construction verification statements will be prepared for chemical agent rooms, laboratories, and containers. (Laboratory hoods, refrigerators, and freezers are exempt from this requirement). The statement will be posted inside each room and laboratory.

13–8. Security lighting

Security lighting will be provided for exterior doors of buildings containing chemical agents to discourage unauthorized entry and to facilitate the detection of intruders attempting to gain entry into the building. Security lighting will also be provided for the entrance doors of rooms or laboratories which contain chemical agents.

13–9. Intrusion detection system (IDS)

a. Rooms or laboratories which store chemical agents will be provided with approved IDS (AR 190–13) to detect unauthorized entry.

b. IDS sensors will also be installed on exterior doors and windows of buildings housing chemical agent rooms or laboratories when the need for such IDS is determined by the site vulnerability assessment.

c. IDS sensors will be installed inside the protected area.

d. IDS control units will be placed inside the chemical agent room/laboratory. If the control unit cannot be placed inside the protected area, the control unit will be secured inside a locked, tamper alarmed, weather proof, container on the outside of the protected area in close proximity to the entrance.

e. IDS will terminate at a manned location with the capabilities to initiate an immediate response by security force personnel as specified in the site physical security plan.

f. IDS will be in secure mode (ready to respond to an intrusion) at all times when the room or laboratory containing chemical agents is unoccupied.

g. Additionally, rooms or laboratories containing chemical agents will be equipped with a volumetric or motion detection sensor system capable of detecting entry and movement of an intruder within the protected area. The sensor

system will be configured to cover all potential approaches to chemical secure containers (for example, laboratory hoods containing chemical agents).

h. Alarm activation will be displayed at the alarm center. Audio and visual indication will show line supervision and access/secure status.

i. Appropriate security measures will be taken when IDS is not operable. The security measures will be established in the site physical security plan.

j. IDS will be provided with backup battery power supply, independent of the primary power source, which will be capable of operating the equipment for 4 hours. A battery charging system and automatic switchover to backup battery power will be provided. Audible and visual indications that primary power has failed or has been restored will also be provided. The battery power supply system will be kept under surveillance or contained in an alarmed cabinet to protect the system against tampering. The backup battery power system will be tested each quarter or more often as recommended by the alarm manufacture.

k. Procedures will be established in the site physical security plan to provide immediate security response to alarms. Alarms will be recorded and retained on file for 1 year. Records will include the nature of the alarm, the date and time the alarm was received, the location, and action taken in response to the alarm. Records will be reviewed by supervisor personnel to ensure proper actions were taken, and to identify and correct IDS reliability problems.

l. IDS sensors will be tested by causing an actual alarm at least every 90 days or more often as recommended by the alarm manufacture. Such alarm activation will include opening doors and deliberate movement within the room or laboratory. Test procedures will simulate expected actions of a potential intruder. Testing will be accomplished by security personnel or by IDS maintenance or laboratory personnel under the supervision and in the presence of security personnel. Where advanced sensor systems which provide the capability to remotely stimulate individual sensors via an electronically activate sensor phenomenology device are installed, this capability may be used to fulfill the quarterly testing requirement.

m. Security personnel or laboratory personnel under the supervision of security personnel will conduct actual test of IDS immediately following maintenance, repair, or modification of IDS, particularly when sensors, wiring, circuits, control units, or alarm status indicators are involved.

n. A record of all tests of IDS sensors and backup battery power system will be maintained for 12 months. The record will reflect the date of the test, the name of the person(s) conducting the test, results of the test, and any required corrective action resulting from the test. All IDS tests and backup battery tests will be recorded in the guard log.

o. Detailed test procedures will be developed and will include sensitivity and performance standards for each sensor.

13–10. Security forces

a. Sufficient armed security forces will be available at all times to respond to attempted penetrations and prevent the unauthorized removal of chemical agents.

b. The actual number of response force personnel will be specified in the facility security plan, based on the postulated and local threats to chemical agents and facility vulnerability assessment.

c. At a minimum, the response time for security forces will not exceed 15 minutes from the time of an intrusion alarm or report of a security incident.

d. Armed security patrols will conduct random, periodic checks of the exterior of the building containing chemical agents when the building is secured for the day. The frequency and types of patrol checks will depend on the threat, vulnerability, and physical layout of the facility, and will be established in the site physical security plan. The rationale for the frequency and types of patrol checks will be documented in the vulnerability assessment and included in the facility security plan. The purpose of such patrols will be to conduct security checks to ensure that the facility is intact and has not been broken into. Exterior doors and windows will be included in the security checks.

e. In addition to the patrols, an armed security patrol will make compensatory security checks of the facility at least every hour when IDS is inoperative and the building housing the room or laboratory is unoccupied or secured for the day.

f. A system of communications adequate to meet unique storage, location, and operating conditions associated with chemical agents will be established for security forces. This will include communications between operating personnel in the chemical agent room or laboratory and response forces.

g. Arming of security force personnel will be subject to the requirements of AR 190–14, including the use of firearms and restrictions on the use of deadly force.

h. Commanders will ensure that security force personnel are trained and capable of performing their duties and are reliable and trustworthy. Training exercises will be conducted monthly. A record of the security force training and respond exercises will be maintained for 1 year.

i. Activities with more than one chemical agent storage area need not establish separate, dedicated security back-up forces unless such action is supported by the site vulnerability assessment. When such forces serve more than one

chemical agent storage area, plans will identify actions to be taken in the event of multiple intrusions. These actions will be exercised at least once every 3 months and will be documented.

13-11. Two-person rule

Access to chemical agents will be controlled according to the two-person rule (see glossary) requirement in AR 50-6.

13-12. Key and lock controls

The key and lock control requirements in chapter 8 apply. Additional guidance is as follows:

- a.* Access to or possession of both keys to installed locks on chemical agent rooms, laboratories, or containers by one person is prohibited. This prohibition will also apply to the locksmith and key control officer.
- b.* Access to or possession of the combination of both locks to chemical agent rooms, laboratories, and containers by one person is prohibited.
- c.* Keys to installed locks on chemical agent rooms/ laboratories or containers will not be removed from the facility.

13-13. Entry controls

Entry controls will be established by commanders to control routine entry and deter unauthorized persons from entering rooms and laboratories where chemical agents are stored or used. Access to such rooms or laboratories by a lone individual will be prohibited. The following requirements apply—

- a.* Warning signs will be posted that the area is subject to special restrictions and controls and that only authorized persons are permitted entry.
- b.* An entry control roster (ECR) of personnel authorized entry will be maintained at the chemical agent room or laboratory concerned. ECRs will contain the name, and identification document number of the photographic ID card used for entry. A state driver's license, Government CAC, or any other government issued photographic ID may be used for this purpose.
- c.* Entry into chemical agent rooms and laboratories will be physically controlled by personnel who are listed on the ECR and assigned to the facility concerned.
- d.* Personnel who control entry into chemical agent rooms and laboratories and preclude unauthorized access are required to be in the PRP. (Chemical agent rooms and laboratories are designated as limited areas according to paragraph 13-2, above.)
- e.* Visitors authorized to enter chemical agent rooms or laboratories will be escorted by personnel who are listed on the ECR and assigned to the facility concerned.
- f.* A register will be maintained to record the entry and exit of visitors.
- g.* A means of rapid communication and an electronic duress system will be provided to personnel controlling entry to rooms and laboratories containing chemical agents to immediately contact security personnel for assistance in case of emergencies.
- h.* A list of names and phone numbers of persons to be contacted in an emergency will be maintained by security personnel.
- i.* Entry control system will also include rapid entry procedures in emergencies.
- j.* Entry and exit control procedures may be modified for Chemical Weapons Treaty Compliance Inspections. There will be strict controls at all times to provide for verification and identity of personnel, escorts, and preclude access to security interests.

13-14. Package and material control

A system of package and material control will be established by commanders. The system will be used to control movement of packages and materials into and out of chemical agent rooms and laboratories. Procedures will be established for inspecting for prohibited items and contraband. Items of particular concern will include unauthorized introduction of weapons and explosives and unauthorized removal of chemical agents. Sealed packages that cannot be inspected will require a signed property pass (OF-7). The bearer of the sealed package will not be authorized to sign the property pass. The property pass will be signed by another authorized person. Persons authorized to sign property passes will be designated in writing by the commander or his designated representative. Samples of signatures of personnel authorized to sign property passes will be maintained at the exit control point. Other packages and materials not covered by a property pass will be inspected for unauthorized items. Package and material control procedures may be modified to meet Chemical Weapons Treaty Compliance Inspections in paragraph 7-7, above.

13-15. End of day security checks

- a.* Commanders will establish a system of security checks at the close of each working day to ensure that rooms and laboratories containing chemical agents are secured.
- b.* Responsible personnel will be designated in writing to conduct checks of all chemical agent containers and doors to chemical agent rooms or laboratories to ensure they are secured.
- c.* Action will be taken to have the IDS systems activated upon leaving the chemical agent room or laboratory.

d. Actions in *a* through *c* above will be recorded. Standard Form 701 (Activity Security Checklist) may be used to meet this requirement. Records will be retained for a period of 30 days.

13–16. Opening of room or laboratory after duty hours

Except in an emergency, covered by the site physical security plan, before a chemical agent room or laboratory is opened after normal working hours, authorization will be obtained from the commander or designated representative. When such an opening is authorized, pertinent facts will be entered in the guard daily log. Each change of shift will review the daily log, including the record of IDS alarms, and, if deemed necessary because of facts and circumstances, verify the validity of such authorization with the commander. Such procedures will be established in the site physical security plan.

13–17. Security inspections

Security inspections will be conducted in accordance with chapter 2 of this regulation.

13–18. Recapture and recovery operations

Planning for recapture and recovery operations will be conducted according to chapter 12.

13–19. Physical security plans

Physical security plans will be developed and prepared according to requirements in chapter 3. A copy of the plan will be maintained at the chemical agent room or laboratory for use of such personnel and review by inspector or compliance personnel.

13–20. Transportation

Transportation policy and escort procedures in AR 50–6 and applicable security requirements in chapter 11 of this regulation will be followed for on-post and off-post movement of category III chemical agents.

Chapter 14

Security Provisions for Contracts and Agreements Involving Category III RDTE Chemical Agents at Off Post Locations

14–1. Category III RDTE chemical agents

a. The security provisions of this chapter will apply to contractual arrangements or other agreements involving the authorized transfer of custody of category III RDTE chemical agents to another Government department, or agency, or to the private sector, for use or storage at off post locations.

b. Security provisions will be incorporated in statements of work.

c. Close coordination among the user, and security, custodian, and contracting officials will be required to ensure that security provisions in this chapter are included in contracts and agreements. The contracts and agreements will include security inspection provisions to ensure compliance with regulatory requirements. A security manager will be appointed by the facility manager in writing to administer the security program for the chemical facility.

d. The security provisions in this chapter will apply to new, modified, and updated contracts and agreements in effect after the publication date of this regulation.

e. Requests for security waivers or exceptions will be granted to contractor-owned, contractor-operated facilities according to provisions in chapter 2.

14–2. Limited and exclusion areas

Chemical agents will be secured in an exclusion area within a limited area. The areas will be designated in the facility security plan according to the following criteria:

a. The limited area will be designated as the inside of a room or laboratory containing a chemical secure container.

b. The exclusion area will be designated as the inside of a chemical secure container.

c. A temporary exclusion area will be designated when chemical agents are removed from the chemical secure container. The temporary exclusion area for this purpose will be the area immediately surrounding the chemical agents. In the absence of positive measures to prevent physical access by unauthorized persons, access to the temporary exclusion area will constitute access to the chemical agents.

14–3. Vulnerability assessment

a. A vulnerability assessment will be prepared in writing for facilities where chemical agents are stored or used. The assessment will be accomplished by a team consisting of the facility security manager, knowledgeable members of the facility security force, or local law enforcement officials, when applicable, and Government security specialists.

b. The DA Implementing Instructions to the DOD Postulated Threat to chemical agents will be provided to the

contractor by the Government. The contractor will use the postulated threat and local threat in conjunction with the facility vulnerability assessment.

c. Vulnerability assessments will be conducted according to requirements in chapter 16 of this regulation. The vulnerability assessments may be modified to conform to the physical layout and surrounding environment of the facility. A copy of this regulation will be provided to the contractor by the Government.

d. The vulnerability assessment will contain the actions taken to counter vulnerabilities identified during the assessment. The contractor will use the standardized format in chapter 16 of this regulation to document the results of the vulnerability assessment.

14-4. Storage/containers

a. Chemical agents will be stored in any of the following chemical secure containers—

- (1) Laboratory hoods, freezers, or refrigerators.
- (2) Locally fabricated containers of at least 20 gauge steel, or material of equivalent strength.
- (3) Built-in containers constructed of at least 20 gauge steel, or material of equivalent strength, mounted in concrete at counter top level.
- (4) Security containers, vaults, safes, or vault-type rooms described in AR 380-5 for storage of classified material (any classification designation).

b. Following requirements will apply to chemical agents stored in laboratory hoods:

- (1) Laboratory hoods with glass will be protected with steel mesh panels with a grid of not more than 1 inch by 2 inches center-to-center that can be raised or moved for authorized access to the chemical agents inside the laboratory hoods. Installation of panels will meet local safety requirements.
- (2) Laboratory hoods that are not protected with steel mesh panels will be stored in locked metal containers inside the laboratory hoods. The metal containers will be securely fastened to the laboratory hood structure.
- (3) Steel mesh panels are not required to be installed on the face of laboratory hoods when the built-in containers are installed inside laboratory hoods.

c. All chemical secure containers, regardless of type, will be secured with two locks. Military specifications for medium security padlocks have been cancelled (see http://locks.nfesc.navy.mil/gfsp_introduction.htm). Medium security padlocks are authorized for continued use to secure all categories III RDTE chemical agents only until local stocks are depleted or replacement is necessary. At a minimum, containers will be secured with two GSA-approved changeable 3-position padlocks built to Federal Specification FF-P-110, or a GSA-approved built-in combination lock, or a mix of two of these types of locks.

d. Hasps and staples for padlocks will be of heavy pattern steel, securely fastened to the structure with smooth head bolts, heavy duty rivets, or welding.

e. Chemical secure containers will be stored in rooms or laboratories meeting specifications outlined in paragraph 14-5, below, of this regulation.

14-5. Rooms and laboratories

The following minimum security construction standards apply to rooms or laboratories containing chemical agents:

a. Walls, floors, and ceilings will be constructed of at least ½-inch plywood, 1-inch tongue-in-groove wall boards or the equivalent. Roofs with suspended ceilings will be protected to ensure the crawl space cannot be used for covert entry.

b. Windows and openings (for example, conduits, vents, and ducts) in excess of 96 square inches with a smallest dimension greater than 6 inches will be barred or grilled to ensure a degree of security comparable to that provided by the walls of the room or laboratory.

c. Doors will be constructed of solid core wood or metal, possess the appropriate UL fire rating, and be designed to complement the security provided by the exterior walls of the rooms and laboratories. Hinges should be mounted inside the room or laboratory, or, if this is not possible, hinges mounted outside such rooms and laboratories will be welded, peened, or brazed to preclude removal from outside the door. Doors not used for primary entrance will be secured from the inside at all times and devoid of external locking hardware. The doors will be equipped with appropriate hardware to permit rapid exit from the room or laboratory in the event of fire or other emergency.

d. Military specifications for medium security padlocks have been cancelled (see http://locks.nfesc.navy.mil/gfsp_introduction.htm). Medium security padlocks are authorized for continued use to secure all categories III RDTE chemical agents only until local stocks are depleted or replacement is necessary. The main entrance door to the chemical agent room or laboratory will be secured with a minimum of two key-operated deadbolt locks (with a one-inch throw), or two GSA-approved changeable three-position padlocks built to Federal Specification FF-P-110, or a GSA-approved built-in combination lock, or a mix of two of these types of locks. Padlocks will be mounted on comparable hasps.

e. All other doors will be locked from the inside with a deadbolt locking device (a minimum of 1 inch throw),

crossbar, or similar barrier resistant to manipulation from the outside. Panic hardware, when required, will be installed so as to prevent opening the door by fish-wire operation of the bolt from outside the door.

14-6. Exterior doors of buildings

Exterior doors of buildings which house rooms or laboratories containing chemical agents will be provided with an appropriate locking device on each door.

14-7. Security construction verification

Security construction verification statements will be prepared for chemical agent rooms, laboratories, and containers (laboratory hoods, refrigerators, and freezers are exempt from this requirement). Qualified technical personnel will verify the construction composition (for example, walls, ceilings, roofs, floors) of the chemical agent rooms and laboratories. The construction verification will be in writing and will be signed and dated by the responsible technician qualified to perform this task. The statement will show whether or not the structures or containers conform to the construction criteria in these security provisions. Any deviations from the construction criteria will be noted. The contractor will be responsible for correcting such deviations. The statement will be on file at the facility and made available for review during security compliance inspections. Construction verification statements will be updated when construction modifications are made.

14-8. Security lighting

Security lighting will be provided for exterior doors of buildings containing chemical agents to discourage unauthorized entry and to facilitate the detection of intruders attempting to gain entry into the building. Security lighting will also be provided for the entrance doors of rooms or laboratories which contain the chemical agents.

14-9. Intrusion detection system (IDS)

- a. Rooms or laboratories which store chemical agents will be provided with IDS to detect unauthorized entry.
- b. The IDS will be designed so that it cannot be defeated by an intruder before producing an alarm.
- c. The IDS sensors will be installed inside the protected area.
- d. The interior of the room or laboratory will be provided with a volumetric or motion detection sensor system capable of detecting entry and movement of an intruder within the protected area. The sensor system will be configured to cover all potential approaches to chemical secure containers (for example, laboratory hoods containing chemical agents).
- e. IDS control units will be fitted with tamper detection devices that annunciate at the alarm monitoring panel, and will be located inside the room or laboratory being protected. When the IDS control unit cannot be placed inside the protected area, the control unit will be secured inside a locked, tamper alarmed, container on the outside of the protected area in close proximity to the entrance. The keys to the IDS control units will be controlled and accounted for at all times.
- f. IDS will be in a secure mode (ready to respond to an intrusion) at all times when the room or laboratory containing chemical agents is unoccupied.
- g. IDS will be provided with backup battery power in case of electric power failure.
- h. Alarm activations for IDS sensors will be displayed at the alarm monitor center. The following requirements will apply:
 - (1) The alarm center will be capable of providing 24-hour alarm signal monitoring service.
 - (2) In the event of an alarm, the system will be capable of locating the zone where the signal on the premises originated.
 - (3) Alarm monitoring personnel will maintain a continuous watch, 24 hours a day, 7 days a week.
 - (4) Alarm monitoring personnel manning a proprietary alarm system will have and maintain the high standards of conduct and reliability expected of law enforcement and security personnel. As a minimum, a favorable review of local police records will be conducted for these personnel prior to their employment. In the case of a non-proprietary alarm system, the contractor will obtain assurance from the security company providing this service that the alarm monitoring personnel have been checked for reliability through a favorable review of local police records.
 - (5) When an alarm is signaled, alarm monitoring personnel will immediately initiate a response to determine the cause of the alarm. Security or local police personnel, as appropriate, will be notified, as well as designated facility personnel. The response actions by all personnel concerned will be included in the facility security plan which will require approval by the Government.
 - (6) When notified of an alarm or incident, the designated facility person will immediately report to the facility to ascertain the nature of the alarm or incident and take appropriate measures to ensure the security of the chemical agents. If the designated person fails to report to the facility, or cannot be contacted for any reason, designated military authorities will be notified promptly to ensure that the required action is taken.
 - (7) Compensatory security measures will be taken immediately when the IDS is inoperable. In the absence of IDS

protection, appropriate surveillance will be provided for all rooms or laboratories in which chemical agents are stored. The security measures will be included in the facility security plan, which will require approval by the Government.

(8) Actions taken in response to alarms or inoperative IDS will be recorded and made available for review.

i. Testing: the following procedures will be followed:

(1) Each IDS sensor will be tested by causing an actual alarm at least quarterly or as often as recommended by the alarm manufacture.

(2) Testing procedures will ensure that IDS sensors meet the intended IDS protection standards for rooms or laboratories containing chemical agents.

(3) IDS sensors will be tested immediately following maintenance, repair, or modification of IDS.

(4) Backup battery power for IDS will be tested at least quarterly or more often as recommended by the manufacture.

(5) Testing will be conducted by designated facility personnel.

(6) Testing procedures will be coordinated between IDS testing personnel at the facility and personnel at the alarm monitor panel to ensure the system is operating satisfactorily.

(7) Testing results for the previous twelve months will be recorded and made available for review.

(8) Testing procedures will be included in the facility security plan.

14–10. Security response forces

a. Sufficient security forces will be available at all times to respond to attempted penetrations and prevent unauthorized removal of chemical agents.

b. The security forces will consist of facility employed guards, contract guards, or local police.

c. The response time for security forces or local police will not exceed 15 minutes from the time of an intrusion alarm or report of a security incident.

d. Security patrols will conduct random, periodic checks of the exterior of the building containing chemical agents when the building is secured for the day. The frequency and types of patrol checks will depend on the threat, vulnerability, and physical layout of the facility. The rationale for the frequency and types of patrol checks will be documented in the vulnerability assessment and included in the facility security plan.

e. When the local police are used to provide a security response to alarms or incidents, or to provide the random, periodic patrol checks of the building containing chemical agents, a Memorandum of Agreement (MOA) between the contractor and local police will detail the police support provided to the facility. The MOA will require approval by the Government, and will be included as part of the facility security plan.

f. The contractor will ensure that security force personnel employed or contracted by the contractor are trained and capable of performing their duties and are reliable, and trustworthy.

g. Arming and use of force restrictions for security personnel who are not law enforcement officials will be subject to the laws of the state and local jurisdictions concerned.

14–11. Communications and duress system

a. A rapid means of communication and an electronic duress system will be provided to laboratory personnel to immediately contact security personnel for assistance in case of emergencies.

b. Security personnel employed or contracted by the facility will have a system of communications commensurate with the security mission and local operating conditions.

14–12. Two-person rule

The two-person rule will apply to access of chemical agents by authorized personnel according to requirements in AR 50–6.

14–13. Key and lock controls

a. Keys to installed locks on chemical agent storage rooms, laboratories, and containers will be strictly controlled at all times. These keys will be maintained separately from other keys and will be accessible only to those individuals whose official duties require access to them. Keys will not be left unattended or unsecured at any time.

b. Access to or possession of both keys to the locks of chemical containers and entry doors to rooms or laboratories containing chemical agents by only one person will be prohibited. The two-person rule in AR 50–6 will apply to keys allowing access to chemical agents. A key control system will be established so that no one will be allowed to interchange access to keys to installed “A” and “B” locks to the rooms, laboratories, or chemical containers.

c. Keys required for maintenance and repair of IDS, including keys to the control unit door and monitor cabinet, will be accessible only to authorized maintenance personnel. A list of authorized maintenance personnel will be kept current and accessible to personnel who control such keys. Testing of IDS by designated facility personnel will be required immediately after maintenance, repairs, or modifications of IDS.

- d.* A roster of personnel authorized to receive keys to storage areas will be kept current. The roster will be signed by the administrative official of the Chemical Personnel Reliability Program.
- e.* The number of keys will be held to a minimum. Master key and keyed alike systems will be prohibited. Keys will not be duplicated unless authorized in writing by the key control officer. Duplicated keys will be strictly accounted for at all times.
- f.* When not attended or used, keys will be secured in a locked key container. Any GSA-approved security container, or equivalent container, or key container of at least 20-gauge steel, will be acceptable for storing such keys. The key container will be located in a room where it is kept under surveillance or in a room that can be locked during non-duty hours. An appropriate locking system will be used to lock the key container. Procedures will be established to preclude access of the stored keys which require two-person control.
- g.* Keys described in this chapter will be accounted for at all times. This requirement will also apply to keys securing the key containers.
- h.* Keys to installed locks in will not be removed from the facility.
- i.* In the event of lost, misplaced, or stolen keys, the affected locks or cores to locks will be replaced immediately. Compromised lock combinations will also be changed immediately.
- j.* Combinations to locks, when used, will be changed—
- (1) When placed in use.
 - (2) When an individual knowing the combination no longer requires it.
 - (3) When the combination has been subject to compromise.
 - (4) At least every 12 months.
- k.* Lock combinations will be recorded, sealed in an envelope, and stored in a security container. No other written record of the combination will be kept. SF-700, (Security Container Information), may be used to record the lock combinations. Controls will be established to ensure envelopes containing combinations to locks are accounted for at all times and not made available to unauthorized personnel. Access to or possession of the combinations of both locks to stored chemical agents by one person will be prohibited.
- l.* Padlocks will be locked to the hasp when the area or container is open to preclude theft, loss, or substitution of the lock.
- m.* Reserve locks and keys will be secured at all times to preclude accessibility to unauthorized personnel.
- n.* Lock location rosters will be protected from unauthorized persons.
- o.* Key control officers and locksmiths will not be authorized access to information concerning the specific locations of installed key operated locks protecting chemical agents at the facility (for example, specific storage container, room, or laboratory). The intent of this requirement is to preclude the possible circumvention of the two-person control system by anyone handling these locks and keys.
- p.* Keys will be inventoried jointly with each change of custody. Keys in two-person controlled containers will be inventoried only when the containers have been opened.
- q.* Not more than every 90 days, a commissioned officer, Department of the Army civilian in the grade of GS-07 or above or a contractor employee in a supervisory position, appointed, in writing, by the commander concerned or designated representative, will inventory keys and locks by serial number. The person appointed to conduct the inventory will not have a vested interest in the outcome of the inventory. Inventories will be reported in writing to the key control officer. Inventories will show the general location of keys and locks, but not the exact location of each installed lock, for example, the specific storage structure involved. Inventory discrepancies will be resolved and reported to the commander concerned. The quarterly inventory requirement does not apply to keys to access/secure switches for IDS control unit doors located inside alarmed chemical agent storage structures. These keys functions as toggle switches to access/secure the IDS when the storage structure is opened and locked. Key inventory records will be kept for 12 months.
- r.* Key control registers will contain the information listed in (1) through (5), below. Completed key registers will be retained in the unit files for at least 90 days. The following will be included in the key control register:
- (1) Serial number. Locks or keys which do not have a serial number will be given one. This number will be inscribed on the lock or key as appropriate.
 - (2) Printed name and signature of the individual receiving the key.
 - (3) Printed name and signature of the person issuing the key.
 - (4) Date and time of issuance, and date and time returned.
 - (5) Printed name and signature of the individual receiving the returned key.
- s.* Padlocks will be changed, have their cylinders replaced, or be rotated randomly between storage structures or facilities at least annually. This requirement will also apply to key padlocks to IDS junction boxes. Such changes will be recorded and retained in the facility files for 1 year.
- t.* The rotation of padlocks will not be required when two locks are installed on each chemical agent structure and a system is set up for separating these locks into “A” and “B” locks. Personnel will be identified and authorized access

only to either “A” or “B” lock keys (or combinations), but not both. The system will preclude an individual from interchanging access to the “A” and “B” keys.

14–14. Key control officer and key custodians

Key control officer’s and key custodian’s duties will be in accordance with chapter 8 of this regulation.

14–15. Entry controls

The contractor will establish written procedures to control routine entry and deter unauthorized persons from entering rooms or laboratories where chemical agents are stored or used. Access to such rooms or laboratories by a lone individual will be prohibited. The following requirements apply—

- a.* Warning signs will be posted that the area is subject to special restrictions and controls and that only authorized persons are permitted entry.
- b.* Only personnel assigned to the facility and authorized routine entry into the chemical agent room or laboratory will be listed on an ECR. Each chemical agent room or laboratory will maintain an ECR which will contain the name, SSN, and organization of assigned personnel. ECRs will be signed by the administrative official of the Chemical Personnel Reliability Program
- c.* Entry into chemical agent rooms or laboratories will be physically controlled by personnel who are listed on the ECR and assigned to the facility concerned.
- d.* Personnel who control entry into chemical agent rooms or laboratories and preclude unauthorized access will be required to be in the PRP.
- e.* Visitors authorized to enter chemical agent rooms or laboratories will be escorted by personnel who are listed on the ECR.
- f.* A register will be maintained to record the entry and exit of visitors.
- g.* A list of names and phone numbers of persons to be contacted in an emergency will be maintained by security personnel.
- h.* Entry and exit control procedures may be modified to meet Chemical Weapons Treaty Compliance Inspection requirements. The procedures will be included in the facility security plan.

14–16. Package and material controls

A system of package and material control will be established by the contractor. The system will be used to control movement of packages and materials into and out of chemical agent rooms or laboratories. Procedures will be established for inspecting for prohibited items and contraband. Items of particular concern will include unauthorized introduction of weapons and explosives and unauthorized removal of chemical agents. Sealed packages that cannot be inspected will require a signed property pass (OF–7). The bearer of the sealed package will not be authorized to sign the property pass. The property pass will be signed by another authorized person. Persons authorized to sign property passes will be designated in writing by the contractor. Samples of signatures of personnel authorized to sign property passes will be maintained at the exit control point. Other packages and materials not covered by a property pass will be inspected for unauthorized items. Package and material control procedures may be modified to meet Chemical Weapons Treaty Compliance requirements.

14–17. End of day security checks

- a.* The contractor will establish a system of security checks at the close of each working day to ensure that rooms and laboratories containing chemical agents are secured.
- b.* Responsible personnel will be designated in writing to conduct checks of all chemical agent containers and doors to chemical agent rooms or laboratories to ensure they are secured.
- c.* Action will be taken to have the IDS systems activated upon leaving the chemical agent room or laboratory.
- d.* Actions in a through c above will be recorded. Standard Form 701 (Activity Security Checklist) may be used to meet this requirement. Records will be retained for a period of 30 days.

14–18. Opening of room or laboratory after working hours

Except in an emergency, covered by the facility security plan, before a chemical agent room or laboratory is opened after normal working hours, authorization will be obtained from the contractor or his or her authorized representative. When such an opening is authorized, the pertinent facts will be documented. Procedures will be established in the facility security plan to provide for responsible facility personnel to challenge the validity of the authorization, when dictated by the facts and circumstances in the case.

14–19. Security inspections

- a.* The security inspection of the contractor’s facility will be conducted by the Government on an annual basis.
- b.* In addition to the annual security inspection, an unannounced security inspection may be conducted by the Government during the life of the contract.

c. The contractor will provide access to prime and subcontractor chemical agent facilities to enable the Government to conduct such inspections, as well as investigations.

d. Security inspectors who are assigned to conduct the security inspections will be trained and qualified to conduct the security inspections according to requirements in AR 190–13, chapter 2.

14–20. Duration of security provisions

The security provisions for chemical agents specified in this chapter will apply for the life of the chemical agents regardless of contract expiration.

14–21. Chemical agent recapture and recovery plan

The Government will provide the contractor with the overall plan and guidance for the recapture and recovery of seized or stolen chemical agents. The contractor will ensure that the Government plan and guidance are integrated with the facility recapture and recovery plan, which will be developed by the contractor with the assistance of Government security personnel. The facility recapture and recovery plan will be coordinated with local law enforcement authorities. The plan will be included in the facility security plan.

14–22. Reporting security incidents

The contractor will report promptly all losses (actual or suspected), or recovery of chemical agents, or any attempt to steal chemical agents, or to damage a chemical agent storage facility, to proper law enforcement authorities. Such incidents will also be reported promptly and directly to the Contracting Officer or representative for additional guidance concerning such incidents. The reporting procedures will be specified in the facility security plan.

14–23. Physical security plan

a. The contractor will prepare a facility physical security plan to implement the security provisions of this contract.

b. The plan will be prepared according to the physical security plan outline in paragraph 14–24, below. The outline may be modified as necessary to facilitate the plan, but all applicable security requirements in the security provisions of this contract will be covered in the plan.

c. The plan will be signed by the contractor, reviewed by a government security representative, and then submitted to the Contracting Officer for approval. The plan will be updated as required, but will be reviewed formally and appropriate changes made at least annually. A copy of the approved plan will be provided to facility security personnel concerned. A copy of the plan will also be maintained at the chemical agent room or laboratory for use of such personnel and review by security inspector personnel.

d. The plan, or portions thereof, will be classified, if required, according to guidance and criteria in AR 380–86, Classification of Chemical Warfare and Chemical and Biological Defense Information, and DOD 5220.22R, Industrial Security Regulation. A copy of AR 380–86 and DOD 5220.22R will be provided to the contractor.

14–24. Physical security plan outline

a. *Name of facility.* Self-explanatory.

b. *Address.* Self-explanatory.

c. *Mission of the facility.* Self-explanatory.

d. *Purpose.* Cite a brief purpose of the plan. In general, the plan should ensure that good planning has integrated all forces, devices, and equipment into an effective security system.

e. *Objectives.* Cite the objectives of the plan.

f. *Threat analysis.* Review DA postulated security threat for chemical agents. Consider local threat assessment based upon the local security officer's evaluation of the threat from terrorism, espionage, sabotage, theft, and vandalism. Persons and organizations threatening or attempting any of these acts will be identified. The threat analysis will be updated at least yearly and more frequently if changing conditions warrant.

g. *Vulnerabilities.* Review results of the facility vulnerability assessment. Identify critical and other structures, containers, buildings, and work areas that require protection. Consider their location, size, function, and contents even if they are only used occasionally.

h. *Priorities.* Establish priorities for protecting various areas within the facility.

i. *Limited and exclusion areas.* Delineate these areas.

j. *Equipment and devices to detect or delay intrusion.*

(1) *Type and construction of storage areas/containers.* Walls, windows, openings, ceilings, and floors of such areas; and containers. Provide estimated delay time for forced entry.

(2) *Security lighting.*

(a) Types.

(b) Locations.

(c) Inspections and maintenance.

(d) Emergency actions for power failure.

- (3) *Protective alarms.*
 - (a) Types.
 - (b) Locations.
 - (c) Monitoring and use.
 - (d) Tests.
 - (e) Inspections and maintenance.
 - (f) Sensitivity settings.
 - (g) Records and logs.
 - (h) Actions by security forces, or local police, and designated facility personnel when alarms occur or when the system, or any part of the system, becomes inoperative.
 - (i) Duress system.
 - (j) Warnings and alarms.
 - (k) Power sources (types and capabilities).
- (4) *Communications systems.*
 - (a) Types.
 - (b) Locations.
 - (c) Use.
 - (d) Tests.
 - (e) Inspections and maintenance.
 - (f) Records/logs.
- (5) *Locks and keys.*
 - (a) Types.
 - (b) Use.
 - (c) Locations.
 - (d) Controls, logs, and accountability.
 - (e) Two-person control keys.
- k. *Measures to control personnel and material.*
 - (1) Personnel access controls.
 - (a) Assigned personnel.
 - (b) Visitors—cleared and uncleared.
 - (c) Maintenance personnel.
 - (2) Escort requirements.
 - (3) Search procedures.
 - (4) Duress system.
 - (5) Non-operational hours access procedures.
 - (6) Emergency entrance procedures. Means of immediate entry for fire, security, disposal, and medical personnel.
- l. *Personnel identification system.* Assigned personnel, visitors, maintenance personnel, and entry control rosters.
 - (1) Identification cards (or personal recognition).
 - (2) Badges, if used.
 - (3) Entry control rosters.
- m. *Material control.*
 - (1) Incoming.
 - (a) Requirements for admission, to include restrictions.
 - (b) Inspection and search.
 - (c) Sealed packages and containers.
 - (2) Outgoing.
 - (a) Documentation required.
 - (b) Inspection and search.
 - (3) Classified documents or materials relevant to this contract or transported in or out of the area.
- n. *Security forces (as applicable).*
 - (1) Type (employee, contract, and local police).
 - (2) Composition and organization.
 - (3) Authority and jurisdiction.
 - (4) Weapons, ammunition, and equipment.
 - (5) Rules of engagement and use of deadly force.
 - (6) Training.

- (7) Information on posts as follows:
 - (a) Locations.
 - (b) Areas of responsibility.
 - (c) Hours.
 - (d) Duties and functions including general patrol routes. Vary patrol routes and times and rotate stationary posts to combat boredom.
 - (e) Reporting procedures.
- (8) Back-up forces—
 - (a) Purpose and mission.
 - (b) Size, composition, and organization.
 - (c) Weapons, ammunition, and equipment.
 - (d) Location and call-out procedures.
 - (e) Reaction time.
 - (f) Training, if applicable.
- o. Emergency actions of general nature.* Actions not covered by this plan which are required for emergencies, such as fire, bomb threats, serious injuries, and so forth.
- p. Movements of chemical agents.* Procedures to ensure security compliance.
- q. Coordination.* Liaison and coordination with cognizant civil agencies, including local police and FBI, as appropriate.
- r. Appendixes.*
 - (1) DA postulated security threat.
 - (2) Local security threat.
 - (3) Vulnerability assessment.
 - (4) Recapture or recovery plan.
 - (5) Guard orders, if applicable.
 - (6) MOA with local police, if applicable.
 - (7) Security incident reporting procedures.
 - (8) Entry and exit procedures for Chemical Weapons Treaty Compliance Inspections.

Chapter 15

Chemical Demilitarization Processing Operations

15-1. All categories of chemical agents

The provisions of this chapter apply to all categories of chemical agents undergoing chemical demilitarization (DEMIL) processing operations. Chemical agents will be protected against sabotage, theft, loss, seizure, or unauthorized access, use, or diversion while undergoing chemical DEMIL processing operations. The protective measures will be required at all times until the termination status of the chemical agents have been established according to AR 50-6. The commander of the storage depot will have overall responsibility for security of all chemical agents on the installation, to include chemical demilitarization operations.

15-2. Movement of chemical agents to chemical DEMIL processing facilities

Movements of chemical agents from established storage sites to chemical DEMIL processing facilities will be conducted in accordance with chapter 11.

15-3. Chemical DEMIL processing facilities

a. All buildings and structures used for DEMIL processing operations with the exception of laboratories that perform analytic testing on DEMIL operations, will be located within a protected limited area consistent with the perimeter security system requirements in chapter 4 (for example, perimeter fences, IDS, clear zones, security lighting, entry control facilities, and so forth).

b. Specific exclusion areas will be designated for chemical agents consistent with DEMIL processing operations. The following are considered exclusion areas when chemical agents are present—

- (1) Areas where chemical agent items are transferred from the transporting vehicles to the unloading docks of the DEMIL facilities. This does not include the Container Handling Building (CHB) when chemical agents are stored inside On-Site Containers (ONC) or Enhanced On-Site Containers (EONC) or Spray Tank shipping containers. The security requirements in paragraph 15-4a (1) and (2) will apply.
- (2) Areas where chemical agent items enter the DEMIL processing system for unpacking.
- (3) Areas where chemical agent items are repositioned to start the DEMIL process system.

(4) Areas and rooms where storage tanks and transfer pipes containing chemical agents are used in the DEMIL processing system.

15-4. Storage/Staging limitations

a. DEMIL plants. Chemical DEMIL processing facilities do not meet security construction standards in chapter 5 for normal storage of chemical agents. The facilities were designed for daily, continual processing of chemical agents in an industrial plant setting. When processing is stopped for operational reasons, or plant operations break down, the facilities may be used for temporary staging of chemical agents pending continuation of processing operations. Examples are processed chemical agents that are stored in the sealed agent storage tanks awaiting incineration in the Liquid Incinerator; chemical agents that have been introduced to processing and cannot be safely retrieved; and chemical agents that are waiting processing and cannot be returned to the storage depot for safety reasons. The following security requirements apply:

(1) When required by operational necessities, unprocessed chemical agent items may be temporarily staged in a properly secured area of the DEMIL facility while waiting DEMIL production.

(2) Unprocessed chemical agent items temporarily staged in the DEMIL facility will be protected at all times against sabotage, theft, loss, seizure, or unauthorized access, use, or diversion.

(3) The duration of the temporary staging of unprocessed chemical agent items will be approved by the commander of the chemical storage activity.

(4) Unprocessed chemical agent items authorized for temporary staging will be protected in a locked area within the DEMIL processing facility.

(5) All doors to the area containing the chemical agents will be protected by an intrusion detection system.

(6) When the area is not occupied by authorized personnel, continual surveillance of the chemical agents will be required by direct visual observation or with the aid of closed circuit television.

(7) Surveillance personnel will immediately notify security response forces in the event of unauthorized access or activities involving the chemical agents.

(8) Personnel responsible for surveillance of the chemical agents will have two types of communications systems to contact security response forces. At least one type of communication will be radio.

(9) Detailed security measures will be in writing and communicated to all personnel concerned. The security measures will be included in guard orders and operator standing operating procedures. Security measures and communication checks will be documented by all personnel concerned and retained on file for one year.

b. Use of ONC/EONC and the Spray Tank Shipping Container. The ONC/EONC and Spray Tank Shipping Container is used to transport chemical agents to the DEMIL facilities on-site. The structural design of the ONC/EONC and Spray Tank Shipping Container provides protection against unauthorized access to chemical agents (additional locking devices are not required), provided compensatory security measures are taken when the loaded ONC/EONC and Spray Tank Shipping Container is unattended. The ONC/EONC and Spray Tank Shipping Container may be used for temporary storage of chemical agents under the following conditions:

(1) *Container handling building (CHB).*

(a) Loaded ONCs may be temporarily stored in the CHB while awaiting conveyance to the unpack area for processing. As a minimum, the following security measures will be followed for loaded ONC/EONC's or Spray Tank Shipping Containers within the CHB.

(b) Chemical Munitions will not be removed from the ONC/EONC or Spray Tank Shipping Containers while positioned within the CHB.

(c) The CHB will be manned 24 hours/7 days a week by a minimum of two CPRP-certified personnel.

(d) Two separate forms of communication will be present in the CHB, that is, radio and telephone with communications checks performed and documented at the beginning of each shift between the CHB and Control Room Operators. Documentation of these checks will be maintained for 12 months.

(e) Closed Circuit Television (CCTV) surveillance camera checks of the CHB will be completed and documented every four hours by control room operator personnel. This documentation will be maintained for a minimum of one year.

(f) CCTV surveillance cameras will scroll continuously on a single monitor within the control room. This scrolling will include views of the CHB along with areas where chemical agent is located in unmanned areas within the Munitions Demilitarization Building (MDB). A dedicated personnel monitor is not required.

(g) For EONC's only, all mobile power sources located in the CHB used for opening the EONC's will be maintained under two-person control when in use and locked in a cabinet or room when not in use. Keys and locks used for this purpose will be controlled and managed as surety keys and locks.

(2) *Reconfiguration building.*

(a) Loaded ONCs may be temporarily staged at the reconfiguration building while waiting processing for removal of explosive fillers from munitions. Since the building will normally be located outside the limited area of the DEMIL facility and chemical storage depot, the building will be protected by a fence and lighting, with entry and exit controls,

and designated as a restricted area according to requirements in AR 190–13. At least two armed guards will be posted in the restricted area to provide security anytime chemical munitions are present inside or outside the building.

(b) Loaded ONCs which remain outside the building while waiting unloading and processing will be kept under direct observation by at least one of the posted armed guards. The ONCs will be positioned in such a manner as to prevent easy access and removal of the bolts securing the ONC door.

(c) Guards will be instructed in writing concerning their required duties and use of deadly force. A reliable system of communications will be provided to ensure rapid communications between posted guards and backup security forces.

(d) A vulnerability assessment will be conducted to determine if additional security measures (for example, more guards, IDS, and so forth) are required to ensure adequate protection of the chemical munitions. The results of the vulnerability assessment will remain on file for review. Security procedures and guard force requirements will be incorporated in the security plan.

15–5. Security of doors and windows

a. Doors will be solid core wood or metal and ensure a level of security equal to or greater than the security provided by the attached walls of the rooms and building. Hinges will be mounted inside the room or building or, if this is not possible, hinges mounted outside such rooms or buildings will be welded, peened, or braised to preclude removal from the outside door.

b. Doors not used for normal entrance will be secured from the inside at all times with a substantial locking bar or dead bolt when the area is unoccupied and be devoid of external locking hardware. Panic hardware, when required, will be installed so as to prevent opening the door by fish-wire operation of the bolt from outside the door.

c. Windows and openings (for example, conduits, vents, and ducts) in excess of 96 square inches with the smallest dimension greater than 6 inches will be barred or grilled to ensure a degree of security equal to or greater than the attached walls of the rooms or the buildings. For operational needs, bar and grill work on ventilation ducts need not be placed at the point of penetration but can be located anywhere within the ductwork or piping.

d. Removable openings (for example, roof and crawl space hatches) will be secured from the inside of the room or building with low security padlocks (NSN 5340–00–158–3805, or NSN 5340–00–158–3807) and comparable hasp or key operated 1-inch throw deadbolt. All doors and removable openings to chemical exclusion areas will have IDS installed.

e. Windows to any exclusion area boundaries, for example along the Observation Corridor of the MDB, do not require rod or bar grillwork. One-quarter inch metal panels may be substituted.

15–6. Locking systems

a. Military specifications for medium security padlocks have been cancelled (see http://locks.nfesc.navy.mil/gfsp_introduction.htm). At a minimum, access doors will be equipped with General Services Administration (GSA) approved changeable three-position padlocks built to Federal Specification FF–P–110, or GSA approved built-in combination lock, or a mix of two of these types of locks. A high security paddock “A” and “B” locking system may be used in lieu of these two combination locks for Exclusion Area Doors providing access into areas where chemical agent is present and undergoing or awaiting demilitarization. Interior doors to enclosures with the Exclusion Area equipped with internally installed panic bars may be secured on the external side of the panic hardware with built in key operated locks to provide rapid access by personnel in PPE.

b. Doors which are not ordinarily used for access will be secured from within according to requirements in paragraph 5–3b.

15–7. Key and lock controls

Key and lock controls will be established according to requirements in chapter 8.

15–8. Interior IDS

Interior IDS will be installed in chemical DEMIL processing facilities in process areas or rooms where chemical agents are present. IDS requirements in paragraph 5–7 apply.

15–9. Monitoring of IDS and CCTV

a. Perimeter IDS and perimeter CCTV will be monitored by security force personnel.

b. CCTV used to monitor plant operations also will be used to monitor security operations within the plant area, particularly those areas where chemical agents are present or undergoing DEMIL processing. The CCTV will be monitored by chemical DEMIL plant personnel.

c. When the capability exists, CCTV security coverage will be monitored by security personnel for security interests. Detailed written procedures, describing all security-related duty responsibilities, will be provided to DEMIL plant personnel performing this monitoring function.

d. Personnel monitoring CCTV will have two types of communications systems to contact security personnel when

required. At least one type of communication will be radio. Detailed written instructions for CCTV monitoring and communications requirements will be provided to all personnel concerned, including security personnel.

15–10. Entry and exit controls

Entry and exit controls in chapter 7 apply.

15–11. Security forces

Security forces requirements in chapter 9 apply.

15–12. Integration of security posture

Security of chemical DEMIL processing facilities will be integrated with security of respective chemical storage sites. The DEMIL Site Program Manager (SPM) is responsible for a Site Facility Security Plan. The Physical Security Plan may be an Annex to the Site Physical Security Plan, or may be a separate plan. The DEMIL Facility Security Plan, either as an annex to the overall Site Security Plan or as a separate plan will be provided to and approved by the MSC.

Chapter 16

Conduct of Vulnerability Assessments and Documentation

16–1. All categories of chemical agents

A vulnerability assessment (VA) will be conducted at each chemical facility and laboratory to—

- a.* Determine the facility's vulnerability to sabotage, theft, loss, seizure, or unauthorized access, use, or diversion of chemical materials from both external and internal threats.
- b.* Counter the identified vulnerabilities.

16–2. The DA Implementing Instructions to the DOD Postulated Threat

The VA team will utilize the DA Implementing Instructions to the DOD Postulated Threat to chemical agents, DA and SMC annual threat statements, when assessing the facility's vulnerabilities.

16–3. Conduct of vulnerability assessment and reviews

- a.* VAs will be conducted:
 - (1) When a chemical facility is activated.
 - (2) When no record exists of a prior VA.
 - (3) When significant changes/modifications to the facility have taken place since the last VA that may impact on the site security posture, that is construction of facilities, loss of intrusion detection systems, and so forth
 - (4) When significant changes have been made to the DA implementing guidance that would impact security forces.
 - (5) When the commander determines greater frequency is required.
- b.* VAs will be formally reviewed annually (every 12 months) and forwarded through command channels for review.
- c.* SMC will ensure chemical facilities complete the required VAs, updates and annual reviews, and submit through command channels, in a timely manner.

16–4. VA team composition

- a.* The VA will be accomplished by a team consisting of the following personnel:
 - (1) Chemical facility commander/director, or representative (commander's/director's participation is encouraged, but is not required).
 - (2) Team leader: the commander concerned will designate the team leader).
 - (3) Chemical facility, installation security specialist, and the DEMIL Facility Security Specialist.
 - (4) Knowledgeable members of the chemical facility.
 - (5) Installation security forces representative.
 - (6) Intelligence community representative.
 - (7) Safety representative and chemical operations subject matter expert.
 - (8) When available the VA team will also include the following personnel to provide technical and professional assistance within their areas of expertise:
 - (a) Security specialists from the headquarters of major subordinate commands or SMC.
 - (b) Other security specialists from outside the span of control of the chemical facility commander.
 - (c) Special forces personnel.
 - (d) Corps of Engineers protective design specialists.
- b.* The VA review and updates will be accomplished by a team consisting of the following personnel —

- (1) Chemical facility and installation security specialist.
- (2) Knowledgeable members of the chemical facility.
- (3) Installation security forces representative.
- (4) Intelligence community representative.

16-5. Annotated outline/guidance for conducting initial VA

a. References:

- (1) DA Implementing Instructions to the DOD postulated threat.
- (2) Army Threat Message used for this review.
- (3) SMC Threat Statement(s) used for this review.

b. Introduction. Provide a brief background of what is to be assessed/evaluated.

c. Purpose. Provide the purpose of the assessment, including what it is to be used for and how it is being applied. Brief all VA team members on the VA purpose and threat to chemical materials. As a minimum, when providing threat briefing, use the DA Implementing Instructions to the DOD postulated threat, Army Threat Message, SMC Threat Statement, and local threat statement.

d. Scope. Describe what facilities are and are not included in this VA. Provide a detailed briefing to team members on each facility assessed. (Maintain briefings on file until the next formal VA is conducted.)

e. Site mission. Provide a brief description of the site mission for each facility.

f. Threat condition. Identify any changes in the postulated or local threat.

g. Site description. Provide a site description and surrounding areas, including maps or photographs. Include photographs when available. Review functional schematics and engineering drawings of facility equipment and structures. The VA team will tour the facility and surrounding area to become knowledgeable of the site configuration, terrain, chemical storage structures, security system, security forces, and technical operational activities at the facility. During the tour, the team will identify specific vulnerabilities from external and internal threats. The team will—

- (1) Observe day and night operations.
- (2) Interview personnel as appropriate.
- (3) Have security equipment and procedures demonstrated.
- (4) Note how the security systems are utilized, to include security forces and backup forces.
- (5) Ask “what if” questions with reference to the possibility of covert or overt acts by insiders. Concentrate on means to bypass, subvert, overwhelm, or interrupt elements in the security systems, or two-person rule.
- (6) As part of the terrain walk around the facility, note the logical avenues of approach, areas providing concealment, fields of fire into the facility, and probable strong points for attackers.

h. Characterization of security systems. Describe the physical protection, access control, and multi-element protection measures in place to protect target locations from the threat spectrum. Characterization should be specific to all protection in place relative to facility targets, exclusion and limited areas. Describe layers of protection and include the condition of security components. Review all facility defense plans and pertinent SOPs.

i. Waivers and exceptions in effect. List all approved waivers and exceptions in effect.

j. Security force status. Describe the composition of security forces, to include authorized and required strength since the last review.

k. Security system components condition. Describe the general condition of security components, that is, vehicle barriers, entry gates, fences, access controls, locks, area lighting, alarms, communication equipment, and protective clothing.

l. Security Interests. Identify specific areas that contain chemical agents and address any security interests that were not considered and why.

m. Scenario development. Identify potential target items in each area. Describe potential adversarial acts for each potential target, that is, sabotage, theft, loss, seizure, unauthorized access, use, or diversion.

n. Identification and description of potential threats. Address what specific threats apply to this site as identified by the DA implementing instructions on threats to chemical facilities based on the DOD postulated threat, Army Threat Message, SMC Threat Statement, and local threat statements. Be specific; state likely threat objectives; threat tactics; and tools, explosives and weapons that the threat could use in execution of their attack. Describe what threats were considered and eliminated and why. Include the following:

- (1) Insider adversaries.
- (2) Outsider (external) adversaries.
- (3) Insider and outsider collusion.
- (4) Airborne attack or penetration.

o. Scenarios developed. Describe in detail the plausible scenarios that were developed for each potential target for the specific threat spectrums.

- (1) Develop and document plausible scenarios for each potential target (paragraph m above).

(2) Develop each scenario by utilizing a two-party, adversary and defender, gaming approach. Together the two parties choose credible paths and actions for the adversaries as well as plausible responses by the security system.

p. Test exercise results. Conduct a test exercise for each identified threat, that is, if insider threat has been identified as a threat to the facility, then conducts an exercise to determine its viability. From these exercises you should be able to determine:

- (1) If the response force (RF) responds within the appropriate time limits.
- (2) If the security systems already in place mitigate the potential threat to an acceptable level.
- (3) Are additional measures required to mitigate the potential threat to an acceptable level?
- (4) Provide a recapitulation of security system probabilities, delay times for chemical storage structure barriers, adversary target task times, security force response times, and security force neutralization times.

q. Conclusions/vulnerabilities and recommendations. State the conclusions and recommendations which were developed during the VA. Conclusions will express results that follow logically from the VA. Recommendations will support conclusions, and will be designed to reduce scenario likelihood of success for each identified vulnerability. State the Commanders concurrence/nonconcurrence, with comments, as appropriate using the following format:

- (1) Conclusion/vulnerabilities.
- (2) Recommendation.
- (3) Commander's concurrence/nonconcurrence (with comment).

r. Commander's decisions on conclusions and recommendations. Provide signed endorsements by each commander in the chain of command.

(1) The commander concerned will make a formal decision on the conclusions and recommendations made by the VA team. Each identified vulnerability and recommended corrective actions will be addressed.

(2) Forward the VA documentation through command channels to the SMC.

(3) Each commander in the chain of command will review and endorse the VA documentation to ensure that appropriate corrective actions are initiated or accomplished.

(4) The SMC Commander or his designated representative (General Officer, or equivalent Senior Executive Service civilian) assigned the responsibility for physical security matters will approve/disapprove all VAs.

16–6. Annotated outline/guidance for conducting annual VA reviews and updates

a. References:

- (1) DA Implementing Instructions to the DOD postulated threat.
- (2) Army Threat Message used for this review.
- (3) SMC Threat Statement(s) used for this review.

b. Threat update. Identify any changes in the postulated or local threat.

c. Waivers or exceptions in effect. List all approved waivers and exceptions in effect.

d. Facility update. Identify any changes to facility operations, staffing, infrastructure, and facilities or in the surrounding area since the last review. List all changes that may have created a new vulnerability.

e. Security force status. List any changes in authorized or assigned strengths and security force structure.

f. Security systems components condition. Describe the general condition of security components that is vehicle barriers, fences, access control points, locks, area lighting, alarms, communications equipment and protective equipment.

g. Security systems status. List any additions, upgrades and/or degradation since the last review.

h. Summary and status of corrective action(s): Review each conclusion/vulnerability identified by the initial VA or subsequent updates and determine status of corrective actions, that is, pending, on-going or closed.

i. New conclusions/vulnerabilities identified. List each conclusion/vulnerability identified as a result of the annual review.

j. Recommendations. Identify corrective actions to mitigate each identified conclusion/vulnerability for each target as a result of the annual review.

k. Commander's decision on conclusions and recommendations. The Commander's overall conclusion for the VA to include each identified vulnerability and corrective action.

Chapter 17

Protective Purposes Production Facility (PPPF) Category III Chemical Defense Training Facility (CDTF)

17–1. Category III CDTF chemical agent general requirements

a. The provisions of this chapter will apply to category III CDTF chemical agents that are produced, secured, used in training or other authorized purposes.

b. Where conflicts exist between the requirement of this chapter and other parts of this regulation, the requirements of this chapter have precedence.

c. Access to chemical agents will be controlled according to the two-person rule (see glossary) requirement in AR 50–6.

17–2. Limited/exclusion areas

Chemical agents will be secured in an exclusion area within a limited area. The areas will be designated in the facility security plan according to the following criteria—

a. The limited area will be designated as the inside of the laboratory where the chemical secure containers are located.

b. The exclusion area will be designated as the inside of a chemical secure container.

c. Temporary Exclusion Area (TEA).

d. A TEA, as defined in AR 50–6, will be established when chemical agents are removed from the chemical secure container and moved into the training areas for the conduct of toxic agent training. The area immediately surrounding the agent carrying container (ACC) will be designated as the TEA and will be under the physical control of two Chemical Personnel Reliability Program (CPRP) certified personnel in accordance with the two person rule of AR 50–6. The TEA is terminated when all CSM in the ACC has been expended or neutralized.

17–3. Vulnerability assessment

A vulnerability assessment will be conducted in accordance with this publication, chapter 16. The vulnerability assessment may be modified to conform to the physical layout and surrounding environment of the facility.

17–4. Storage containers

Chemical agents will be stored in any of the following chemical secure containers:

a. Locally fabricated containers with a minimum of 20-gauge steel, or material of equivalent strength.

b. Built-in containers constructed with a minimum of 20-gauge steel, or material of equivalent strength, mounted in concrete at counter top level.

c. All chemical secure containers, regardless of type, will be secured with two high security locks.

d. Hasps and staples for padlocks will be a minimum of 3.0 mm steel, securely fastened to the structure with smooth head bolts, heavy duty rivets, or welding.

e. Chemical secure containers will be stored in rooms or laboratories, which meet the security construction standards in this publication, paragraph 17–5, below.

17–5. Laboratory (limited area)

a. Construction of the limited area must meet the following minimum criteria:

(1) Walls, floors, and ceilings will be constructed of concrete.

(2) Exterior openings (for example, windows, conduits, vents, and ducts) in excess of 96 square inches with the smallest dimension greater than 6 inches will be covered with a minimum of 9 gauge wire in a 2-inch diamond pattern.

(3) Doors will be constructed of solid core wood or metal, and be designed to complement the security provided by the exterior walls of the laboratory. Hinges should be mounted inside the room or will be tamper resistant, welded, peened, brazed, or shrouded to preclude removal of the door.

b. The main entrance door to the laboratory will be secured with two high security locks, that is key operated deadbolts with minimum 1” throw, high security padlocks mounted on high security hasps, or a combination of locks meeting the requirements for high security as approved by the DOD lock program office.

c. Doors not used for primary entrance will be secured in accordance with chapter 5, paragraph 5–3b.

17–6. Exterior doors of buildings

Exterior doors of the building which houses the laboratory containing chemical agents will, at a minimum, be provided with a key operated mortise locking device as approved by the DOD lock program.

17–7. Security construction verification

Security construction verification statements will be prepared according to paragraph 5–5 for laboratory and locally fabricated chemical security containers. A copy of the security construction verification will be posted inside the laboratory.

17–8. Perimeter security

The perimeter security system for the CDTF will be established to deter unauthorized entry of an intruder(s) into the restricted area and to enable the security force to execute the appropriate response.

a. Concept. Perimeter fence will be used to clearly delineate and impede entry into the restricted area. When the permanent perimeter fence is not available for any reason, compensatory measures will be implemented.

b. Fencing. A single perimeter fence will protect the CDTF. The perimeter fence will be located with consideration to required clear zones, terrain features, property lines, and building layouts.

c. Fence specifications. The fence will meet the standards and specifications described in U.S. Army Corps of Engineers (USACE) Standard Design Drawing (STD) 872-90-04 for non-sensored fence and have seven foot high fabric (FE-7 fence) plus outriggers. Additional requirements are as follows—

(1) *Vehicle barrier.* A vehicle barrier system of sufficient strength to preclude vehicle penetration into the CDTF restricted area will be installed outside the fence where topography permits high-speed approach.

(2) *Soil-stabilization.* Ground surfaces will be made stable in areas where the sand, shifting soils, or surface water may cause erosion and thereby assist an intruder in penetrating the perimeter security system. Where surface stabilizing is not possible or practical, concrete curbs, sills, or other similar type anchoring devices extending below ground level will be used.

(3) *Gates.* The perimeter fence will have vehicular and pedestrian gates consistent with operational requirements. Gates will be designed so that traffic through them will be under the positive control of the security force. Gates will be closed and secured when not in use. Gates will be structurally comparable and provide the same resistance to penetration as the contiguous fence. Gates will be equipped with appropriate barbed wire toppings (that is , outriggers or vertical arm brackets). The bottom of the gate will be close enough to firm ground to prevent an intruder from crawling under the gate.

(4) *Drainage openings.* Drainage structures, water passages, and other openings penetrating the perimeter fence will be barred to prevent penetration. Openings to drainage structures having a cross-sectional area greater than 96 square inches and the smallest dimension greater than 6 inches will be protected with a minimum of 9 gauge wire in a 2-inch diamond pattern. Covers to manholes of drainage structures penetrating the perimeter fence will be spot-welded closed to prevent opening.

17-9. Clear zones

The purpose of clear zones is to deny protection and concealment to intruders. The following requirements will apply—

a. Clear zones will extend a minimum of 20 feet on both sides of the fence.

b. Clear zones will be clear of all obstacles, topographical features, and vegetation, which could reduce the effectiveness of the perimeter fence (for either ingress or egress), impede assessment, or provide cover and concealment for an intruder.

(1) If clear zones are impractical to maintain because of serious continuing erosion problems or other factors, appropriate security measure will be used. Security measures will compensate for clear zone terrain features or obstacles that may provide areas for intruders to hide in, offer intruder protection from security force weapons, or serve as assembly points for attacking forces.

(2) Perimeter light poles, fire hydrants, steam pipes, or similar objects, and entry control buildings, which are within the clear zone and represent no aid to counter the purpose of the perimeter fence or preclude assessment, do not violate the requirements of a clear zone. Perimeter light and utility poles that can potentially aid in circumventing the fences will be provided with physical barriers.

17-10. Security lighting

Security lighting will be provided to discourage unauthorized entry and to facilitate the detection of intruders approaching or attempting to gain entry into the restricted area. Security lighting will be used during hours of darkness and reduced visibility. The following requirements will apply:

a. Perimeter lighting.

(1) Perimeter lighting will be positioned and designed to enable the detection of persons in the entire clear zone.

(2) When CCTV is used as a means of perimeter assessment, lighting may be varied as needed to accommodate the operation of the CCTV or other electronic imaging systems.

b. Exterior doors. Security lighting will illuminate exterior doors. Switches for exterior lights will be installed so they are not accessible to unauthorized persons. Exterior lights will be covered with wire mesh screen or vandal resistant lenses to protect the lights from being broken by thrown objects.

c. Restart capability. The site security lighting system will have a restart capability of 3 minutes after primary or emergency power is applied.

(1) Emergency power will be provided by an emergency generator.

(2) Generator maintenance and operating procedures will be conducted in accordance with manufactures guidelines.

d. Perimeter lighting circuits. Perimeter lighting circuits will be designed so that failure of one or more lights will not affect operation of the remaining lights.

e. Control of site security lighting. The site security force will be provided a means of controlling site security lighting. Perimeter lighting controls will be installed in the site access center.

17-11. Site Access Center (SAC)

The SAC will control the entry and exit of authorized personnel and vehicles onto the site. This facility may be part of the perimeter security system and will be the point from which personnel and vehicle control operations will be conducted. The facility will include exterior lighting, a covered and lighted structure to permit personnel and vehicle identification inspection during hours of darkness and in any weather condition. The basic makeup of the SAC will include a gatehouse, a personnel entry gate, and a vehicle entry area to include a covered Sally Port.

a. SAC gatehouse. The SAC gatehouse will be constructed to afford protection to security force personnel from small arms fire. Provisions will be made to enable security personnel under duress to transmit an electronic signal discreetly to the installation MP station. The SAC may contain the IDS control center and the perimeter visual-assessment system.

b. Personnel entry area. The personnel entry area will be designed to ensure that personnel entering or exiting the site are under the positive control of security force (for example, by remotely operated gate, door, and so forth.)

c. Vehicle entry area. The vehicle entry area will consist of two gates that are capable of operating independently. Both portal gates will be constructed or modified to incorporate a positive locking feature when closed. An electrically operated gate will have a capability to be manually operated in the event of malfunction or other emergencies. During an emergency or operational requirement, both gates may be opened simultaneously.

d. Vehicle crash barriers. Vehicle crash barriers may be installed at both the inner and outer gates to reinforce the vehicle entry area.

17-12. Perimeter detection and assessment system

Early detection and near real-time assessment are essential for a prompt and effective response by security forces to any attempts to penetrate the site perimeter. The CDTF perimeter will be monitored using a combination of active patrolling, video surveillance, or other appropriate detection and assessment techniques.

a. Imaging systems. Imaging systems provide a remote visual image of activity in an area under surveillance. Acceptable imaging systems such as digital video motion (behavior) detection (DVMD), closed-circuit television (CCTV), including infrared and thermal imagery may be used.

b. Protection of monitor station. The primary monitor station used for visual assessment will be located in an area that is protected against small arms fire.

c. Perimeter road. A perimeter roadway will encompass the entire CDTF on the outside of the perimeter fence. Imaging systems may be used to assist motor or foot patrols on the perimeter roadway in the conduct of security assessments.

17-13. Restricted area designation

a. Commanders of military installations and facilities have the authority to publish and enforce regulations for safeguarding personnel, facilities and property. This authority is derived from Internal Security Act of 1950 (50 United States Code (U.S.C.) 797), and is implemented by DODD 5200.8, Security of DOD installations and Resources and DOD 5200.8-R, Department of Defense Physical Security Program.

b. The Garrison commander will designate CDTF Site as a restricted area in accordance with AR 190-13.

c. Post signs or notices in conspicuous and appropriate places to identify a restricted area (except when such action would tend to advertise an otherwise concealed area, or when in conflict with Host Nation Agreements). Position signs so not to provide concealment of an intruder or obstruct visual assessment.

d. Signs will read: THIS ACTIVITY HAS BEEN DECLARED A RESTRICTED AREA BY AUTHORITY OF THE OF THE INSTALLATION COMMANDER IN ACCORDANCE WITH THE PROVISIONS OF THE DIRECTIVE ISSUED BY THE SECRETARY OF DEFENSE ON 24 April 1991, PUSUANT TO THE PROVISIONS OF SECTION 21, INTERNAL SECURITY ACT OF 1950. UNAUTHORIZED ENTRY IS PROHIBITED. ALL PERSONS AND VEHICLES ENTERING HEREIN ARE LIABLE TO SEARCH. PHOTOGRAPHY OF THE FACILITIES IS PROHIBITED WITHOUT SPECIFIC AUTHORIZATION FROM THE COMMANDER. DEADLY FORCE IS AUTHORIZED.

e. Existing signs containing essentially the same wording as in DEF 872-90-01 may continue to be used until replacement is necessary at which time the required wording in DEF 872-90-01 will be used.

17-14. Intrusion detection system (IDS)

a. The laboratory that stores chemical agents will be provided with approved IDS to detect unauthorized entry. See AR 190-13 for IDS standards and procurement procedures.

b. IDS sensors will also be installed on exterior doors and windows of buildings housing the laboratory.

c. IDS sensors will be installed inside the protected area.

d. IDS control units will be placed inside the protected area. If the control unit cannot be placed inside the protected area, the control unit will be secured inside a locked, tamper alarmed, weather proof, container on the outside of the protected area in close proximity to the entrance.

- e.* IDS will terminate at a manned location with the capabilities to initiate an immediate response by on-site security force personnel as specified in the site physical security plan.
- f.* IDS will be in secure mode (ready to respond to an intrusion) at all times when the room or laboratory containing chemical agents is unoccupied.
- g.* Alarm activation will be displayed at the alarm center. Audio and visual indication will show line supervision and access/secure status. Capability will be provided to conduct a remote self-test of the IDS circuit continuity.
- h.* Appropriate security measures will be taken when IDS is not operable. The security measures will be established in the site physical security plan.
- i.* IDS will be provided with backup battery power supply, independent of the primary power source, which will be capable of operating the equipment for 4 hours. A battery charging system and automatic switchover to backup battery power will be provided. Audible and visual indications that primary power has failed or has been restored will also be provided. The battery power supply system will be kept under surveillance or contained in an alarmed cabinet to protect the system against tampering. The backup battery power system will be tested each quarter or more often as recommended by the alarm manufacture.
- j.* Each change of shift of security personnel will ensure that a remote self-test of IDS circuit continuity is conducted at the manned alarm panel. The tests will be recorded in the guard log.
- k.* Procedures will be established in the site physical security plan to provide immediate visual assessment of alarms. Immediate visual assessment is defined within 5 minutes of alarm notification. Alarms will be recorded and the records will be retained on file for 12 months. Records will include the nature of the alarm, the date and time the alarm was received, the location, and action taken in response to the alarm.
- l.* IDS sensors will be tested by causing an actual alarm at least quarterly or more often as recommended by the alarm manufacture. Such alarm activation will include opening doors and deliberate movement within the room or laboratory.
- m.* Security personnel will conduct actual test of IDS immediately following maintenance, repair, or modification of IDS, particularly when sensors, wiring, circuits, control units, or alarm status indicators are involved.
- n.* Test procedures will simulate expected actions of a potential intruder. Testing will be accomplished by IDS trained security personnel or by IDS maintenance personnel under the supervision and in the presence of IDS trained security personnel. Where advanced sensor systems which provide the capability to remotely stimulate individual sensors via an electronically activate sensor phenomenology device are installed, this capability may be used to fulfill the quarterly testing requirement.
- o.* Detailed test procedures will be developed and will include sensitivity and performance standards for each type of sensor.
- p.* A record of all tests of IDS sensors and backup battery power system will be maintained for 12 months. The record will reflect the date of the test, the name of the person(s) conducting the test, results of the test, and any required corrective action resulting from the test. All IDS tests and backup battery tests will be recorded in the guard log.

17–15. Security forces

- a.* As a minimum, two-armed security personnel will be on site at all times.
- b.* The actual number of additional response force personnel will be specified in the facility security plan based on the postulated and local threats to chemical agents and facility vulnerability assessment.
- c.* The response time for security forces to visually assess will not exceed 5 minutes from the time of an intrusion alarm or the report of a security incident.
- d.* Armed security patrols will conduct random, periodic checks of the exterior of the building containing chemical agents when the building is secured for the day. The frequency and types of patrol checks will depend on the threat, vulnerability, and physical layout of the facility, and will be established in the site physical security plan. The rationale for the frequency and types of patrol checks will be documented in the vulnerability assessment and included in the facility security plan. The purpose of such patrols will be to conduct security checks to ensure that the facility is intact and has not been broken into. Exterior doors and windows will be included in the security checks.
- e.* A communications system will be established that is sufficient for communications with the installation Emergency Operations Center, Military Police, response forces and internal organization consistent with the mission of the CDTF to protect CSM. As a minimum, communications should consist of telephone and handheld radios.
- f.* Arming of security force personnel will be subject to the requirements of AR 190–14, including the use of firearms and restrictions on the use of deadly force (AR 190–59, para 2–2b).
- g.* Commander/Director will ensure that security force personnel are trained and capable of performing their duties and are reliable and trustworthy. Installation Response Force exercises will be conducted monthly; a record of the response force exercises will be maintained for 12 months.
- h.* CDTF guard training outline will be used for guard training. Training standards will conform to the performance – oriented tasks, conditions, and standards, supporting skills and knowledge to include performance measures contained

in Training Circular 19-138. As a minimum all security guards will be trained and qualified in accordance with AR 190-56 and on the following subject areas/tasks:

- (1) Initial/basic security guard training.
 - (a) Control entry and exit of a restricted area.
 - (b) Response to alarms.
 - (c) Key and lock control.
 - (d) Intrusion detection system.
 - (e) Use of force to include deadly force.
 - (f) Defensive tactics.
 - (g) Weapons training
 - (h) Side arm qualification.
 - (i) Shotgun familiarization.
 - (j) CDTF Physical Security Plan.
- (2) Annual refresher/continuing training is required on all initial and Basic Security Guard Training subjects.

17-16. Key and lock controls

The key and lock control requirements in chapter 8 apply.

17-17. Entry controls

a. General. Only authorized personnel will be permitted entry into restricted areas. Control procedures will assure positive identification of all personnel prior to entry. Identification may be written or by personal recognition. An armed forces or government issued identification card containing a photograph and sufficient identification data may be used to satisfy the written identification requirement. The following systems and procedures will be incorporated in the CDTF entry control program:

(1) A practical, positive system to identify and control personnel entering, departing, and moving within restricted area.

- (2) An electronic duress system.
- (3) Package and vehicle inspection system.
- (4) Emergency entry procedures.

b. Limited and exclusion area access. Entry to the limited area and exclusion.

c. Area (EA) will be authorized through the use of an entry control roster (ECR). ECRs will have an expiration date and will contain the name and identification document number of personnel authorized to enter. The Director/Commander or Designated Representative will sign all ECRs.

d. Entry controller. Personnel who physically control entry into a limited and exclusion area and preclude unauthorized access are required to be in the CPRP, and listed on an ECR. An entry register will be maintained to record the entry and exit of all personnel entering the laboratory. Record of entry will be maintained on file for 12 months. A means of rapid communication and an electronic duress system will be provided to immediately contact security personnel for assistance in case of emergencies.

e. Entry and exit control procedures. Entry and exit control procedures may be modified for chemical weapons treaty compliance inspections. There will be strict controls at all times to provide for verification and identify of personnel, escorts, and preclude access to security interests.

17-18. Chemical Agent Recapture and Recovery Operations Planning

a. Provisions. The provisions of this chapter apply to all categories of chemical agents.

b. Recapture. Recapture refers to regaining custody of chemical agents which are in the possession of unauthorized persons. In this situation the chemical agents are assumed to be within a limited or exclusion area either in a storage structure or in the open.

c. Recovery. Recovery refers to locating, if necessary, and to regaining the custody and control of chemical agents which have been captured and removed from custodial control.

d. Procedures.

(1) In the event of capture or removal of chemical agents by unauthorized persons, plans will be maintained for the recapture or recovery of the chemical agents.

(2) All necessary actions, including the use of deadly force, will be taken to recapture or recover chemical agents. Actions to recapture or recover chemical agents will be taken promptly or immediately upon availability of needed resources.

(3) The presence of hostages will not deter the taking of decisive action to prevent unauthorized access to or capture or removal of chemical agents. The welfare and safety of any hostages will be considered in determining specific actions to take, but in all instances, the security of chemical agents will be paramount.

e. Planning.

(1) The SMC, with chemical agent custodial or storage responsibilities, will develop and publish overall plans and guidance for the recapture and recovery of seized or stolen chemical agents. Plans will include forces to be used and rules of engagement. Incident reporting procedures will also be included. MACOMs will ensure such plans and guidance are integrated with each facility plan.

(2) Recapture and recovery plans will be prepared for each chemical storage facility. Plans will include specific actions to take, procedures to follow, personnel required, tactics, and weapons to use for all likely situations or scenarios for the site and chemical agents concerned. Coordination with local law enforcement agencies will be included in such plans.

(3) Each chemical storage facility location will conduct annual recapture training for security forces. Recovery operations plans will be exercised according to MACOM guidance.

(4) Information copies of all recapture and recovery plans will be forwarded to the SMC

f. Secure voice radio. Secure voice radio requirements in paragraph 6-4d, above, apply for missions involving chemical agent recovery operations.

Appendix A

References

Section I

Required Publications

AR 50–6

Nuclear and Chemical Weapons and Material Chemical Surety. (Cited in paras 1–1a, 1–1b, 1–1j(4), 2–5b(6), 2–6c, 2–9, 2–10a, 8–2a, 11–1, 11–2a, 11–3, 11–6, 11–5a, 13–11, 13–20, 14–12, 14–13b, 15–1e, 17–1c, and 17–2d..)

AR 190–11

Physical Security of Arms, Ammunition, and Explosives. (Cited in para 5–6b.)

AR 190–13

The Army Physical Security Program. (Cited in paras 2–4, 3–4a, 4–7c, 4–7b, 5–7, 7–2c(1), 7–2c(3), 13–9a, 13–9a, 14–19d, and 15–4 b(2), 17–13b, and 17–14a.)

AR 190–14

Carrying of Firearms and Use of Force for Law Enforcement and Security Duties. (Cited in paras 2–3b, 9–5c, 13–10g, and 17–15f.)

AR 190–40

Serious Incident Report (Cited in para 1–40l(4).)

190–56

The Army Civilian Police and Security Guard Program. (Cited in paras 9–2, 9–5, 10–2, 10–8 b, and 17–15h.)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication.

AR 5–9

Area Support Responsibilities

AR 15–6

Procedures for Investigating Officers and Boards of Officers

AR 25–2

Information Assurance

AR 200–1

Environmental Protection and Enhancement

AR 200–2

Environmental Effects of Army Actions

AR 380–5

Department of the Army Information Security Program

AR 381–10

U.S. Army Intelligence Activities

AR 385–40

Accident Reporting and Records

AR 525–13

Antiterrorism

AR 530-1

Operations Security (OPSEC)

AR 600-8-14

Identification Cards for Members of the Uniformed Services, Their Family Members, and Other Eligible Personnel.

Army Threat Statement

Note: This document may be requested from the Office of the Provost Marshal General (DAPM-MPD-PS), 2800 Army Pentagon, Washington, DC 20310-2800

DA Implementing Instructions to the DOD Postulated Threat

Note: This document may be requested from the Office of the Provost Marshal General (DAPM-MPD-PS), 2800 Army Pentagon, Washington, DC 20310-2800

DA Pam 350-38

Standards in Weapons Training (Available at: www.atsc.army.mil/atmd/strac.)

DA Pam 750-8

The Army Maintenance Management System (TAMMS) Users Manual

DOD 5220.22R

Industrial Security Regulation (Available at: <http://www.dtic.mil/whs/directives>.)

DOD Directive 5210.65

Chemical Agent Security Program (Available at: <http://www.dtic.mil/whs/directives>.)

DOD 5200.8-R

Physical Security Program (Available at: <http://www.dtic.mil/whs/directives>.)

DOD 6055.9-STD

Ammunition and Explosives Safety Standards (Available at: <http://www.dtic.mil/whs/directives>.)

DODD 5200.8

Security of DOD Installations and Resources (Available at: <http://www.dtic.mil/whs/directives>.)

DODD 5200.8-R

Physical Security Program (Available at: <http://www.dtic.mil/whs/directives>.)

Executive Order (EO) 12333

United States Intelligence Activities (Available at: http://www.ncs.gov/library/policy_docs/eo_12333.pdf.)

Federal Specification FF-P-110

Padlock, Changeable Combination (Available at: <http://www.dtic.mil/whs/directives>.)

Field Manual (FM) 3-19.30

Physical Security (Available at: <http://www.train.army.mil>.)

Field Manual (FM) 5-0

Army Planning and Orders Production

MIL-DTL-29181C

Hasp, Shrouded, for High Security Padlock (Available at: <http://locks.nfesc.navy.mil/Links1.html>.)

MIL-DTL-43607

Padlock, Key Operated, High Security (<http://locks.nfesc.navy.mil/Links1.html>.)

Senior Mission Commander (SMC) Threat Statement

Note: May be obtained from the appropriate SMC Commander.

Training Circular (TC) 19-138

Civilian Law Enforcement and Security Officer Training (Available at: <http://www.train.army.mil>.)

USACE Drawing 872-50-01

Barriers (Available at: <http://www.usace.army.mil>.)

USACE Drawing 872-90-1

Restricted Area Perimeter Warning Signs (Available at: <http://www.usace.army.mil>.)

USACE Standard (STD) Drawing 872-90-04

FE7 Chain-Link Security Fence Details for Non-sensored Fence. (Available at: <http://www.usace.army.mil>.)

USACE Standard (STD) Drawing 872-90-05

FE7 Chain-Link Security Fence Details for Sensored Fence (Available at: <http://www.usace.army.mil>.)

50 USC 797

Internal Security Act of 1950 (Available at: <http://www.gpoaccess.gov/uscode>.)

Section III**Prescribed Forms**

This section contains no entries

Section IV**Referenced Forms****DA Form 2062**

Hand Receipt/Annex Number

DA Form 2404

Equipment Inspection and Maintenance Worksheet

DA Form 4604-R

Security Construction Statement

DA Form 4930-R

Alarm/Intrusion Detection Record

DA Form 5513-R

Key Control Register and Inventory

DD Form 577

Signature Card

OF-7

Individual Property Pass

SF Form 700

Security Container Information

SF Form 701

Activity Security Checklist

Glossary

Section I Abbreviations

ACC

Agent carrying container

AF

Augmentation force

AMC

U.S. Army Materiel Command

AOC

U.S. Army Operations Center

BSAT

Biological select agent and toxins

CCTV

Closed circuit television

Chemical-PRP

Chemical Personnel Reliability Program

CHB

Container handling building

CG

Commanding general

COE

Corps of Engineers

CW

Chemical weapons

CPRP

Chemical Personnel Reliability Program

DA

Department of the Army

DCSI

Deputy Chief of Staff for Intelligence

DCSOPS

Deputy Chief of Staff for Operations and Plans

DEMIL

Demilitarization

DOD

Department of Defense

DSN

Defense Switch Network

DTRA

Defense Threat Reduction Agency

ECF

Entry control facility

ECR

Entry control roster/explosive containment room

EONC

Enhanced on-site containers

FBI

Federal Bureau of Investigation

FORSCOM

U.S. Army Forces Command

GSA

General Services Administration

HQDA

Headquarters, Department of the Army

IDS

Intrusion detection system

I,L&E

Installations, logistics and environment

IRP

Individual Reliability Program

JCS

Joint Chiefs of Staff

KCO

Key control officer

MACOM

Major Army command

MDB

Munitions demilitarization building

NAC

National Agency Check

NAR/FAR

Nuisance alarm rates/false alarm rates

NSN

National stock number

OCE

Office of the Chief of Engineers

ONC

On-site container

OPCW

Organization for the Prohibition of Chemical Weapons

OPLAN

Operations plan

OPSEC

Operations security

PIN

Personal identification number

PMG

Provost Marshal General

PPE

personal protective equipment

PRP

Personnel Reliability Program

RDA

Research, development, and acquisition

RDTE

research, development, test, and evaluation

RF

Response force

ROI

Report of investigation

SIR

Serious incident report

SMC

Senior Mission Commander

SOP

Standing operating procedures

SSCC

Site security control center

STD

Standard

TEA

Temporary exclusion area

UL

Underwriter's Laboratory

USACE

U.S. Army Corps of Engineers

USACIDC

U.S. Army Criminal Investigation Command

VAs

Vulnerability assessments

Section II

Terms

Access

Close physical proximity to a chemical agent, container, or munitions under circumstances that could provide an opportunity to acquire, release, tamper with, damage, or come in direct contact with the chemical agent.

Armed

Equipped with a loaded firearm.

Augmentation force

Additional personnel (or units) organized, trained, armed, equipped, and capable of augmenting site security forces as required.

Auxiliary power source

See emergency power source

Barrier

A coordinated series of obstacles designed or employed to canalize, direct, restrict, delay, or stop the movement of an intruding force.

Binary chemical munitions

Defined in AR 50–6 as munitions designed or employed to canalize, direct, restrict, delay, or stop the movement of an intruding force.

Binary munitions components

Defined in AR 50–6 as the parts which form the binary munitions and contain the binary precursors. When assembled, they become category I chemical agent material under the Army Chemical Surety Program.

Binary precursors

Defined in AR 50–6 as the chemicals that combine to produce binary chemical agents.

Category I

Chemical agents as components of weapon systems which contain munitions or explosives, are in bulk form, or contained in binary chemical munitions loaded with both components in rockets, land mines, one ton containers (nerve agents), projectiles and mortars, bombs, binary munitions or intermediates with both components uploaded or located together. Other chemical agents as components of chemical weapons systems which contain explosives. Agent filled spray tanks.

Category II

All other chemical agents including bulk non-nerve agents stored in one ton containers less those items described below.

Category III

All research chemical agent quantities and concentrations that exceed the chemical surety threshold quantity levels (Table 10–2, chap 10, AR 50–6) and RDTE dilute solutions (Table 10–1, chap 10, AR 50–6) authorized for use in RDTE projects, surveillance programs, intelligence evaluation, or scheduled training programs.

Chemical personnel reliability program

Defined in AR 50–6 as an integral component of the Army Chemical Surety Program designed to ensure the highest standards of individual reliability in personnel occupying chemical duty positions.

Chemical secure container

A container, receptacle, or device used to store chemical agents, located within a limited area and secured with approved locking devices.

Clear zone

An area adjacent to a physical barrier (for example, perimeter fences), clear of all objects that could conceal or shield an individual. Clear zones will extend 30 feet on both sides of the perimeter fence when a single fence is used. When

two fences are used, clear zones will extend 30 feet outside of the outer fence, the entire area between fences, and 30 feet inside the inner fence.

Custody

Defined in AR 50–6 as responsibility for the control of, transfer and movement of, and access to chemical agent material. Custody may or may not include accountability.

Deadly force

Defined in AR 190–14 as force that a person uses causing, or that a person knows, or should know, will create a substantial risk of causing death or serious bodily harm. Deadly force will be used only as set forth in chapter 3 of AR 190–14.

Delay

The effort achieved by physical features, technical devices, or security measures and forces that impedes an adversary from gaining access to chemical agents. Normally expressed as a function of time, it is a major consideration in the design and development of chemical agent security systems.

Demilitarization

Defined in AR 50–6 as the mutilation, destruction, or neutralization of chemical agent material, rendering it harmless and ineffectual for military purposes.

Duty officer

A designated duty officer who is not part of the on-site security force.

Duress system

A method by which personnel who control entry into, vouch for, or escort visitors into a limited and/or exclusion area can covertly communicate a situation of duress to other operating or security personnel.

Emergency power source

A separate and distinct source of power, internal to the facility, and in addition to the facility's primary electrical power source, normally an engine generator (also called a standby generator).

Entry control facility

A facility which is part of the perimeter security system and is the point from which personnel and vehicle control and badge operations are conducted.

Exception

An approved permanent continuation of a deviation from this regulation in which the requirements are not being met and the approving authority determines it is inappropriate to meet the requirements. Compensatory security measures are required to provide adequate security for the deviation.

Exclusion area

The area immediately surrounding one or more receptacles containing chemical agents. Normally, the boundaries of an exclusion area are the walls, floor, and ceiling of a storage structure, chemical secure container, or a barrier that establishes the boundary of the exclusion area (such as an igloo or fence). The inside of a chemical secure container is an exclusion area. In the absence of positive preventive measures, access into the exclusion area constitutes access to the chemical agent.

Facility

See site.

Insider

An individual authorized access to or working in close proximity to chemical agents who may be working alone or in collusion with an outside threat group.

Intrusion detection system

A security system consisting of a sensor(s) capable of detecting one or more types of phenomena, signal media, enunciator(s), and energy source, for signaling the entry or attempted entry of a person or other target into the area protected by the system.

Key control officer

A person, other than a locksmith or key custodian, appointed by the commander in writing to manage the lock and key program for the installation or facility.

Key custodian

A person, other than a locksmith or key control officer, who has custody of the keys in use at a particular site or facility.

Keyed alike system

A system that allows a number of locks to be operated by the same key.

King Tut block

A specially designed large concrete block which is placed in front of an igloo or magazine entrance with a fork lift. Access to the igloo or magazine therefore requires a fork lift to move the block. The King Tut block is of sufficient weight to prevent removal without a fork lift.

Limited area

A designated area immediately surrounding one or more exclusion areas. Normally, the area is between the boundaries of the exclusion areas and the inner fence, or the inside of a room or laboratory room where chemical agents are in use or stored.

Memorandum of Agreement

A prescribed format for documenting mutually agreed to commitments.

Near-real time assessment

Instantaneous assessment of the actual cause for the activation of the sensor alarm by either direct visual assessment, or with the aid of electro-optical imaging equipment such as closed circuit television.

Operations security

The protection of military operations and activities resulting from the identification and subsequent elimination or control of intelligence indicators (vulnerabilities) that are susceptible to hostile exploitation.

Postulated security threat

An estimate of the potential adversary types, acts, capabilities, and combinations thereof that could constitute a risk to a facility or asset. A postulated threat is necessary when a specific threat cannot be determined or when an existing threat may change or grow during the projected life cycle of an asset or system faster than security improvements can be developed and implemented. The postulated threat allows for the consideration of future growth in adversary capabilities and is used as the basis for the design of security systems, equipment, and facilities.

Primary electric power source

The source of power, either external (commercial) or internal, that provides power to the site facilities on a day-to-day basis.

Response force

The immediate, on-location security force organized, trained, armed, equipped, and capable of responding to any security situation as required.

Responsible commander

Normally, the first commander in the chain of command who is responsible for the overall security of the chemical agent storage site. (Also referred to as the site commander)

Restricted area

Defined in AR 190–13 as any area to which entry is subject to special restrictions or control for security reasons or to safeguard property or material.

Senior Mission Commander (SMC)

For the purpose of this regulation, the SMC is the Commander, Army Material Command or Commander, Training and Doctrine Command or Commander, Army Test and Evaluation Command, or Commander, Medical Command.

Site

A storage facility, activity, place, or location containing chemical agents.

Site commander

See responsible commander.

Site security control center

A facility from which the site sentries and response forces are controlled. This facility may include the alarm center, the visual assessment facilities, and other appropriate security capabilities.

Small arms fire

Projectiles of the ball type with impact force equal to a 7.62 mm bullet fired from an M14 rifle or equivalent at its highest velocity using service ammunition.

Standby power source

See emergency power source.

Two-person rule

Defined in AR 50–6 as a system designed to prohibit access by an individual to chemical agents by requiring the presence at all performing first aid in case of exposure to chemical agents or to detect incorrect or unauthorized procedures with respect to the task being performed. Each person must be familiar with applicable safety and security requirements.

Visitor

A person who is not permanently assigned for duty at the storage site proper.

Vulnerability assessment

A systematic evaluation process to determine the site's vulnerability to sabotage, theft, loss, seizure, or unauthorized access, use, or diversion of chemical agents from both external and insider threats.

Waiver

An approved temporary continuation of a deviation from this regulation in which the requirements are not being met, pending corrective actions to conform to the requirement. Compensatory security measures are required to provide adequate security for the deviation until corrected.

Section III**Special Abbreviations and Terms**

This section contains no entries.

UNCLASSIFIED

PIN 068953-000

USAPD

ELECTRONIC PUBLISHING SYSTEM
OneCol FORMATTER WIN32 Version 235

PIN: 068953-000

DATE: 08-31-06

TIME: 11:53:11

PAGES SET: 73

DATA FILE: C:\wincomp\r190-59.fil

DOCUMENT: AR 190-59

SECURITY: UNCLASSIFIED

DOC STATUS: REVISION